BlackBerry Enterprise Mobility Server

Installation Guide

3.6

Contents

About this guide.....5

What is BEMS?.....6

Preinstallation checklists..... 8

Example of a large BEMS deployment.....8
Example of a small BEMS deployment.....9
BlackBerry Push Notifications (Mail).....10
BlackBerry Connect and BlackBerry Presence..... 14
BlackBerry Docs..... 21

Installation and upgrade.....24

Supported installation and upgrade paths.....24
Best practices: Preparing to upgrade.....24
Steps to install BEMS..... 24
BEMS setup application modes.....24
Steps to upgrade BEMS.....25
Steps to upgrade BEMS and change to an alternate JRE..... 25
Steps to install BEMS instances into a cluster..... 26

Prerequisites: Installing and configuring BEMS.....28

Core requirements.....28
System and network requirements..... 28
Setting up a Windows service account for BEMS.....31
Database requirements..... 33
Configure the Java Runtime Environment..... 33
Prerequisites: Connect for Skype for Business..... 33
Preparing the computer that hosts BEMS for use with Skype for Business..... 34
BlackBerry Connect service database requirements..... 35
Preparing the Skype for Business topology for BEMS..... 35
SSL certificate requirements for Skype for Business..... 39
Presence prerequisites: Skype for Business.....44
Prerequisites: BlackBerry Push Notifications service..... 45
Grant application impersonation permission to the service account.....45
Microsoft Exchange Autodiscover..... 46
BlackBerry Push Notifications database requirements..... 46
Prerequisites: Cisco Unified Communications Manager IM and Presence Service requirements for Presence..... 47
Create an Application User..... 47
Create a Dummy User..... 48
Configure Cisco Unified Communications Manager and Cisco IM and Presence certificates with the enterprise certificate authority.....48

Prerequisites: Docs service.....50
Server software and operating system requirements.....50
Prerequisites: BlackBerry Directory Lookup, BlackBerry Follow-Me, and BlackBerry Certificate Lookup services.....51

Installing or upgrading the BEMS software.....52
Install the BEMS software.....52
Upgrade BEMS.....56
Perform a Silent Install or Upgrade.....58

Removing the BEMS software.....59
Remove the BEMS software.....59
In a BlackBerry UEM environment, remove the BEMS server references from the BlackBerry Dynamics connectivity profile.....59
In a Good Control environment, remove the BEMS server references for BlackBerry Work.....60
Remove the BEMS Connect server references for BlackBerry Connect.....60

Troubleshooting BEMS installation or upgrade.....62

Appendices.....63
Appendix: AlwaysOn Availability support for SQL Server.....63
Steps to setup SQL Server for AlwaysOn availability.....63
Configure the BEMS services databases for AlwaysOn availability.....63
Enabling AlwaysOn availability group failover to subnets for the BEMS-Core and Mail services.....64
Enabling AlwaysOn availability group failover to subnets for the Connect service.....64
Enabling AlwaysOn availability group failover to subnets for the Docs service.....64
Architecture: BEMS notification flow using the Microsoft Graph API.....64
Architecture: BEMS.....66

Legal notice.....68

About this guide

This guide describes how to install BEMS in your environment.

Note: For ease of following the instructions in this guide, you should use the suggested database names.

This guide is intended for senior and junior IT professionals who are responsible for installing BEMS.

Before using this guide, make sure that you read the following guides for your environment:

BlackBerry UEM environments

- For information about sizing your environment for BEMS and determining whether you should install the BEMS services on separate servers, see the BlackBerry UEM Planning content.
- For information about the BEMS architecture in a BlackBerry UEM environment, see the BlackBerry UEM architecture and data flows content.
- For information about how BEMS notifications flow using Microsoft Graph, see BEMS notification flow using the Microsoft Graph API.
- For information about configuring your environment for disaster recovery, see the Disaster recovery content.
- For information about getting started with BlackBerry Dynamics in a BlackBerry UEM environment, see the BlackBerry Dynamics Administration content.

Good Control environments

- For information about moving or migrating from a Good Control environment to a BlackBerry UEM environment, see the BlackBerry UEM Planning content.
- For information about the BEMS architecture in a Good Control environment, see Architecture: BEMS.

What is BEMS?

BEMS provides additional services for BlackBerry Dynamics apps. BEMS integrates the following services: BlackBerry Mail, BlackBerry Connect, BlackBerry Presence, and BlackBerry Docs. When these services are integrated, users can communicate with each other using secure instant messaging, view real-time presence status of users in BlackBerry Dynamics apps, and access, synchronize, and share work file server and Microsoft SharePoint. The following table describes the services offered by BEMS.

Service	Description
BlackBerry Mail (BlackBerry Push Notifications)	The BlackBerry Mail service accepts push registration requests from devices, such as iOS and Android, and then communicates with Microsoft Exchange Server using its Microsoft Exchange Web Services protocol to monitor the user's enterprise mailbox for changes.
BlackBerry Connect	The BlackBerry Connect service boosts user communication and collaboration with secure instant messaging, corporate directory lookup, and user presence from an easy-to-use interface on IT-provisioned devices.
BlackBerry Presence	The BlackBerry Presence service provides real-time presence status to BlackBerry Work, BlackBerry Dynamics Launcher, and third-party BlackBerry Dynamics applications—giving them a powerful add-in for mobile collaboration.
BlackBerry Docs	The BlackBerry Docs service lets your mobile workers access, synchronize, and share documents natively using their enterprise file server, SharePoint, Box, and content management systems supporting CMIS, without the need for VPN software, firewall reconfiguration, or duplicate data stores.
BlackBerry Directory Lookup	The BlackBerry Directory Lookup service provides users the ability to look up first name, last name, and picture from your company directory and display it within the BlackBerry Dynamics Launcher and other BlackBerry Dynamics apps such as BlackBerry Connect.
BlackBerry Follow-Me	The BlackBerry Follow-Me service keeps the BlackBerry Dynamics Launcher synchronized across multiple devices.
BlackBerry Certificate Lookup	The BlackBerry Certificate Lookup service retrieves S/MIME digital certificates from the user's Microsoft Active Directory account and matches the requested key usage. Only the recipient's public certificate is retrieved for matching.

The BEMS Dashboard is a browser-based administration console which you use to configure the server components and services after the installation completes. The BEMS Web Console, also browser-based, provides real-time monitoring and logging of device connectivity, traffic load, and throughput in near real-time.

Services, in the context of BlackBerry Dynamics, refers to concrete business-level functionality that can be consumed by a plurality of BlackBerry Dynamics applications. For example, "Look up this contact in the directory," "Subscribe to Presence for these contacts," and "Save this file to SharePoint." The BlackBerry Dynamics Services Framework allows client applications on an authenticated device to discover and utilize services by providing

API publication, as well as life cycle and visibility management of services using the BlackBerry Developers For Enterprise Apps.

Preinstallation checklists

Verify that the requirements for the following BEMS services are met before you install BEMS.

- BlackBerry Push Notifications (BlackBerry Mail)
- BlackBerry Connect and BlackBerry Presence
- BlackBerry Docs

You can download the BEMS software from the BlackBerry Products and Application Support. To allow users in your environment to use the latest features available with BEMS, it is recommended that you upgrade your BEMS instances and BlackBerry Dynamics apps on user devices to the latest software versions.

Important: BEMS installations are supported only on English implementations of the operating system.

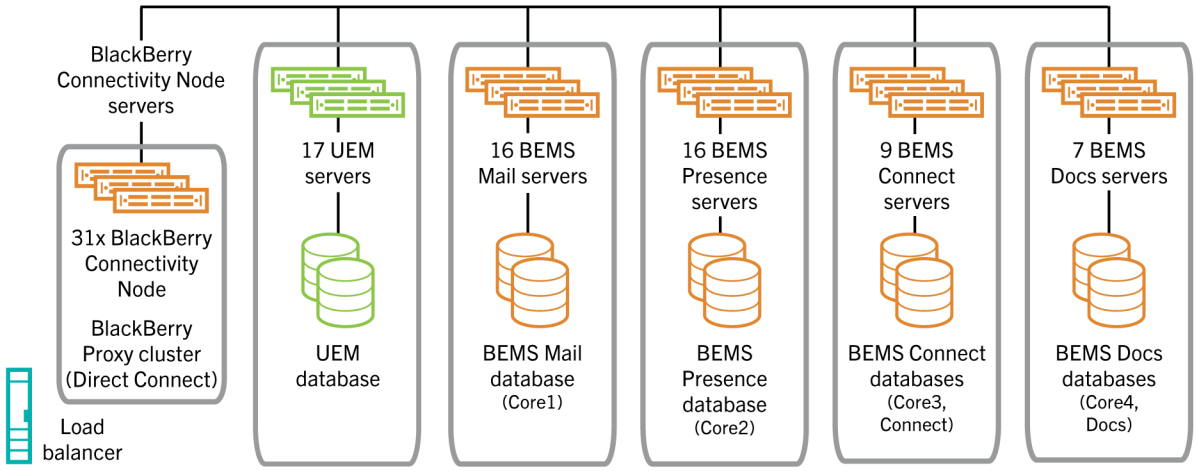
When you verify requirements in this document, see the BEMS Compatibility Matrix.

Note: For ease of following the instructions in this guide, we recommend you use the suggested database names.

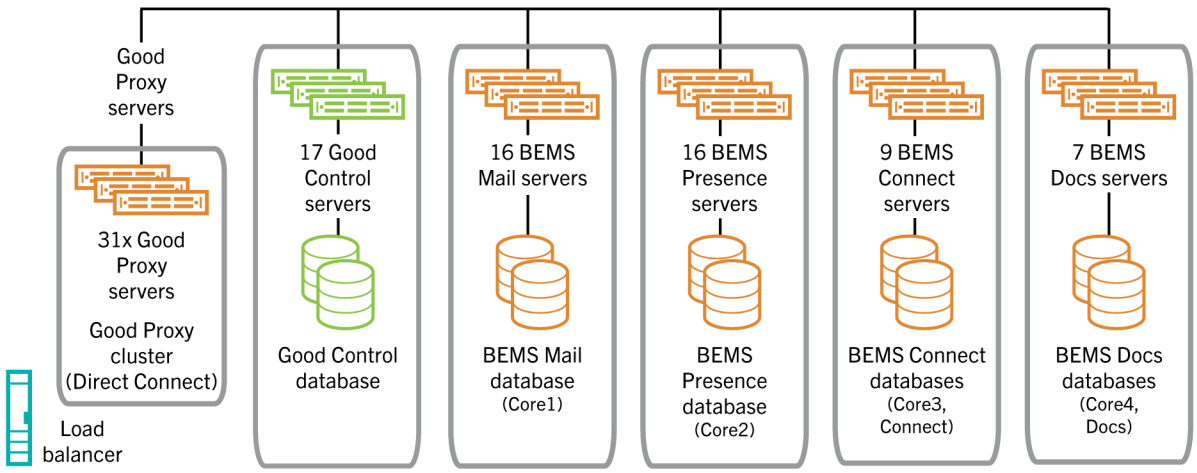
Example of a large BEMS deployment

Below is an example of a large deployment of BEMS with all of the services installed on separate servers.

BlackBerry UEM environment



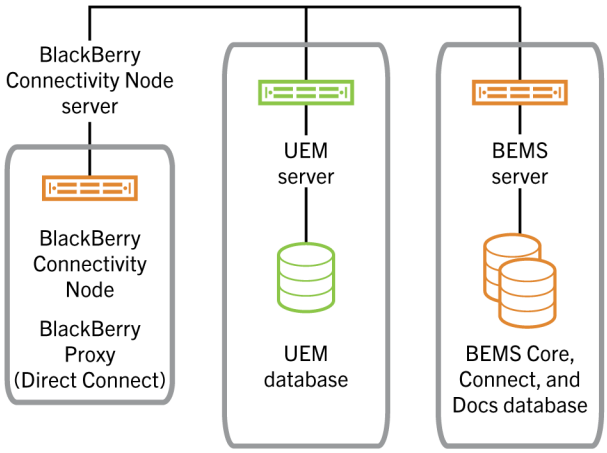
Good Control environment



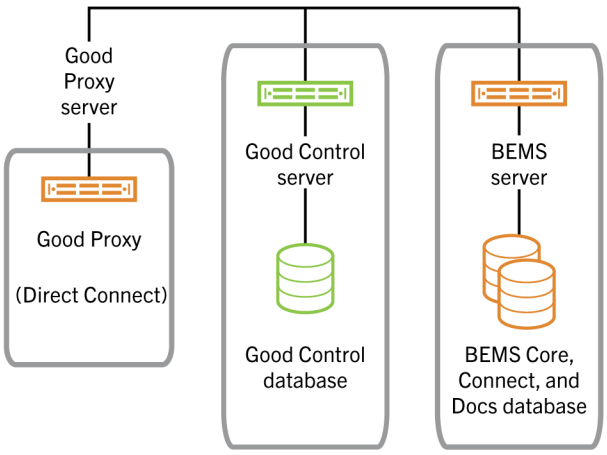
Example of a small BEMS deployment

Below is an example of a small deployment of BEMS with all of the services installed on one server.

BlackBerry UEM environment



Good Control environment



BlackBerry Push Notifications (Mail)

The following requirements apply when you need to configure servers to support BEMS with the BlackBerry Push Notifications (BlackBerry Mail) service in your organization. The BlackBerry Mail (Push Notifications) service accepts push registration requests from devices, such as iOS and Android, and then monitors the user's enterprise mailbox for changes. When changes occur, such as new email, notifications are pushed to devices.

Complete	Requirement
Registration	
☐	Request the BlackBerry Work app from the Marketplace for Enterprise Software portal.
☐	Log in to https://account.blackberry.com/a/organization//entitlements and confirm that you have the appropriate entitlements. For more information about entitlements, see "Configure BlackBerry Work connection settings" in the BlackBerry Work administration content.
Network	

Complete	Requirement

☐	Verify that the following ports are open for BEMS:
	Inbound TCP ports
	• 61616 or 61617 (SSL) to and from servers that host BEMS in the same cluster (bidirectional)
	• 8443 from the BlackBerry Proxy or Good Proxy server (required for Presence and Push Notifications), and optionally for Microsoft Graph for Push Notifications to the reverse proxy server appliance. For more information about how Microsoft Graph communicates with BEMS, see Architecture: BEMS notification flow using the Microsoft Graph API.
	  • If your environment uses Microsoft Graph, you can complete the following:
	  • Restrict the firewall to only accept connections from Microsoft's list of IP addresses. For more information on the available Microsoft Graph Change notifications IP addresses, see https://docs.microsoft.com/en-us/microsoft-365/enterprise/additional-office365-ip-addresses-and-urls?view=o365-worldwide.
	  • Restrict the reverse proxy server to only proxy the /notificationClient URI (for example, *bems_server_name*.example.com:443/notificationClient" ;="bems.example.com:8443/notificationClient BEMS_Pool"
	  • If the reverse proxy appliance is installed in a DMZ, make sure that port 8443 is open from the reverse proxy to each BEMS node.
	Outbound TCP ports
	• 80 to Microsoft Exchange Server (AutoDiscover)
	• 389 and 636 (SSL) to LDAP and 3268 and 3269 (SSL) to Global catalog server
	• 443 to BlackBerry Dynamics NOC (includes connections to APNS)
	• 443 to Firebase Cloud Messaging (FCM)
	• 443 to Microsoft Exchange Server (Microsoft Exchange Web Services, AutoDiscover), optionally 443 to Microsoft Graph
	• 17080 to the BlackBerry Proxy or Good Proxy server (17433 for SSL)
	• 61616 or 61617 (SSL) to and from servers that host BEMS in the same cluster (bidirectional)
	Note: If you use custom ports, make sure that they are open.

Microsoft Active Directory, Microsoft Exchange, and Microsoft Office 365	
☐	Verify that you have a mail server that supports BEMS.
☐	Create a Microsoft Active Directory account for the BEMS service account. For example, BEMSAdmin. For password considerations, see Creating a Microsoft Active Directory account for the BEMS service account.
☐	Grant Application Impersonation Permissions to the BEMSAdmin account in Microsoft Exchange. For instructions, see Grant application impersonation permission to the service account.

Complete	Requirement
☐	Make sure that your Microsoft Exchange Autodiscover is set up correctly. For more information on how to to use third-party tools to test autodiscover, visit support.blackberry.com/community to read article 40351.
☐	Make sure that Microsoft Exchange Web Services (EWS) is enabled on port 443, and that connections are permitted from the BEMS server.
☐	For BEMS environments that use Microsoft Graph, create a public DNS entry for each BEMS cluster. The DNS entry must point to the reverse proxy appliance. The public DNS entry is used as the "External Notification URL" in the BEMS Dashboard when you use Microsoft Graph and Configure BEMS to communicate with a Microsoft Office 365 environment using Microsoft Graph API.
☐	Make sure that your Microsoft Exchange ActiveSync environment is updated to support TLS 1.2. For more information, visit support.blackberry.com/community to read article 56869. If the TLS version is not updated, Push Notifications fail.
Microsoft .NET Framework	
☐	Verify the version of Microsoft .NET Framework. For more information, see Preparing the computer that hosts BEMS for use with Skype for Business.
BEMS	
☐	Verify that your environment is running one of the following: • A version of BlackBerry UEM that supports BEMS. For instructions on installing or upgrading BlackBerry UEM, see the BlackBerry UEM Installation and Upgrade content. • A BlackBerry Dynamics server that supports BEMS. **Important**: The BlackBerry Dynamics server must already be installed and operational before installing BEMS.
☐	Verify that your server is running an operating system that supports BEMS. For information about the supported operating systems, see the BEMS Compatibility Matrix.
☐	Verify that you have the required hardware to host BEMS. For more information about hardware, see one of the following: • In a BlackBerry UEM environment, see BlackBerry UEM Planning content. • In a Good Control environment, see the Good Secure Enterprise Suite Planning content. If you configure your environment for disaster recovery, see the Disaster recovery content.
☐	Make sure that the BEMS service account is a local administrator on the server.
☐	Make sure that the BEMS service account has "Log on as a service" permission.
☐	Verify that the servers that host and access the BEMS Dashboard have a supported browser installed.

Complete	Requirement
☐	Make sure that the server's date and time are set correctly.
☐	Make sure that the server has been joined to the domain.
☐	Make sure that the Windows Firewall is disabled.
☐	Disable antivirus programs before you install or upgrade the BEMS software.
☐	Verify that you have installed JRE 8 on the servers where you will install BEMS and that you have an environment variable that points to its location. For instructions, see Configure the Java Runtime Environment. For information about supported JRE versions, see the BEMS Compatibility Matrix.
☐	Make sure you have connectivity to SQL Server. Typically this is through TCP port 1433.
☐	Ensure connectivity to Microsoft Exchange Web Services (EWS). For more information on how to use third-party tools to test connectivity, visit support.blackberry.com/community to read article 40351.
Database	
☐	Verify that your environment has a database server that supports BEMS. To configure remote TCP/IP connections for Microsoft SQL Server Express, see BlackBerry Push Notifications database requirements.
☐	Make sure that your Microsoft SQL Server environment is updated to support TLS 1.2 if database connection encryption is used. If the TLS version is not updated, you receive an error message and can't access the BEMS dashboard. For more information, visit support.blackberry.com/community to read articles 56869 and 56865.

<table>
<tr><th>Complete</th><th>Requirement</th></tr>
<tr><td>☐</td><td>Depending on the configuration of your environment (for example, all BEMS services on one server or on separate servers), you might need to create one or more SQL Server databases.

The following table is an example of a small deployment that has all of the BEMS services installed on one server. For an example of a large and small deployment that has all of the BEMS services installed on one server, see Example of a small BEMS deployment.

<table><tr><th>Services</th><th>Databases</th></tr><tr><td>All BEMS services on the same server</td><td>Create a database for the BlackBerry Push Notifications service and call it "BEMS_Core".

Note: If this is the first server in the BEMS cluster, create the database. If this is an additional server for the same BEMS cluster, then a new database is not required. Record the existing database name for the BEMS-Core and Mail cluster.</td></tr></table>
The following table is an example of a large deployment that has the BEMS services installed on separate servers. When you create a separate database, you are creating a new cluster for the push notifications. The push notifications are included in the Core database. If you create separate databases, make sure you select the appropriate database for the service. For an example of a large deployment that has the BEMS services installed on separate servers, see Example of a large BEMS deployment.

<table><tr><th>Services</th><th>Databases</th></tr><tr><td>BlackBerry Push Notifications service (Mail service) on one server</td><td>Create a database and call it "BEMS_Core1".</td></tr></table></td></tr>
<tr><td>☐</td><td>Make sure that the Microsoft SQL Server account or the BEMS Windows service account has db_owner privileges to the database. For more information, visit support.blackberry.com/community to read article 42661.</td></tr>
</table>

BlackBerry Connect and BlackBerry Presence

The following requirements apply when you need to configure servers to support BEMS with the BlackBerry Connect and BlackBerry Presence services.

Complete	Requirement
Registration	
☐	Request the BlackBerry Connect app from the Marketplace for Enterprise Software portal.

Complete	Requirement
☐	Log in to https://account.blackberry.com/a/organization//entitlements and confirm that you have the appropriate entitlements. For more information about entitlements, see the following: • BlackBerry Connect entitlements: see "Make BlackBerry Connect available to users in BlackBerry UEM" in the BlackBerry Connect administration content. • BlackBerry Work entitlements: see "Configure BlackBerry Work connection settings" in the BlackBerry Work administration content.
Network: Skype for Business	

	Verify that the following ports are open for BEMS:
	Inbound TCP Ports
	• 8080 or 8082 from the BlackBerry Proxy or Good Proxy server (for BlackBerry Connect
	Note: By default, SSL communication is enabled with a new BEMS 2.12.5.6 or later installation and is bound to port 8082. If you upgraded from BEMS 2.10 or earlier and SSL communication with the BlackBerry Connect app is not enabled, use port 8080. For more information on configuring BlackBerry Connect, see one of the following:
	  • In a BlackBerry UEM environment, see "Configure BlackBerry Connect app settings in BlackBerry UEM" in the BlackBerry Connect administration content.
	  • In a Good Control environment, see "Configure BlackBerry Connect app settings in Good Control" in the BlackBerry Connect administration content.
	• 8443 from the BlackBerry Proxy or Good Proxy server (for BlackBerry Presence)
	• 49555 from the on-premises Skype for Business server (for BlackBerry Connect) when the Connect service is trusted by Skype for Business
	• 49777 from the on-premises Skype for Business (for BlackBerry Presence)
	Outbound TCP Ports
	• 443 to the BlackBerry Dynamics NOC
	• In a Skype for Business on-premises using non-trusted application mode environment, 443 to the following:
	  • lyncdiscoverInternal.<*DomainName*>.com
	  • Fully qualified domain name of the internal Skype Front End pool
	• 206.124.114.0/24
	• 206.124.121.0/24
	• 206.124.122.0/24
	• 5061 (for BlackBerry Connect) to the on-premises Skype for Business server configured as trusted mode
	• 17080 or 17433 to the BlackBerry Proxy or Good Proxy server
	• 1433 to the Microsoft SQL Server (default)
	• 1434 UDP to the on-premises Skype for Business database (for initial setup only)
	• 49152 – 57500 TCP: Random port in this range to the Skype for Business database (for initial setup only)

Complete	Requirement
☐	If your environment uses Skype for Business using non-trusted application mode, verify that at least one DNS entry exists for lyncdiscoverinternal. For more information about DNS requirements for Skype for Business, see https://docs.microsoft.com/en-us/skypeforbusiness/plan-your-deployment/network-requirements/dns.
☐	If BEMS requires a proxy server for external access, record it here: • Proxy server make and model: _____ • Method: _____
Network: Cisco Unified Communications Manager and Cisco IM and Presence	
☐	Verify that the following ports are open for BEMS: **Inbound TCP Ports** 8080 or 8082 from the BlackBerry Proxy or Good Proxy server (for BlackBerry Connect) **Note:** By default, SSL communication is enabled with a new BEMS 2.12.5.6 or later installation and is bound to port 8082. If you upgraded from BEMS 2.10 or earlier and SSL communication with the BlackBerry Connect app is not enabled, use port 8080. For more information on configuring BlackBerry Connect, see one of the following: • In a BlackBerry UEM environment, see "Configure BlackBerry Connect app settings in BlackBerry UEM" in the BlackBerry Connect administration content. • In a Good Control environment, see "Configure BlackBerry Connect app settings in Good Control" in the BlackBerry Connect administration content. **Outbound TCP Ports** • 443 to the BlackBerry Dynamics NOC • 206.124.114.0/24 • 206.124.121.0/24 • 206.124.122.0/24 • 8443 to the Cisco User Data Service • 5222 to the Cisco Jabber XMPP Service • 8083 to the Cisco IM and Presence Service • 17080 or 17433 to the BlackBerry Proxy or Good Proxy server • 1433 to the Microsoft SQL Server server (default)
☐	If BEMS requires a proxy server for external access, record it here: • Proxy server make and model: _____ • Method: _____
Microsoft Active Directory: Skype for Business and Microsoft Exchange	

Complete	Requirement
☐	Create a Microsoft Active Directory service account for the BEMS software (can be the same account used for BlackBerry Push Notifications. For example, BEMSAdmin). The service account must be in the same Microsoft Active Directory domain as the BEMS. For more information, visit support.blackberry.com/community to read article 63703. For account and password considerations, see Creating a Microsoft Active Directory account for the BEMS service account.
☐	Create a mailbox for the BEMSAdmin account.
☐	Grant Application Impersonation Permissions to the BEMSAdmin account in Microsoft Exchange. For instructions, see Grant application impersonation permission to the service account. **Note:** You must mailbox-enable the BEMS-Connect service in Microsoft Exchange to allow the BEMS-Connect service to properly write to the user's conversation history. For specific instructions, see the documentation for the Microsoft Exchange Server version that you are using.
☐	Verify that the BEMS service account has RTCUniversalReadOnlyAdmins permission during the BEMS installation. This permission is granted in the Microsoft Active Directory.
☐	If your environment uses multiple Skype for Business on-premises servers using trusted application mode or non-trusted application mode, have the Skype for Business servers load balanced with a load balance server. For more information about load balancing requirements, visit https://docs.microsoft.com/en-us/skypeforbusiness/plan-your-deployment/network-requirements/load-balancing.
Microsoft Active Directory: Cisco Unified Communications Manager and Cisco IM and Presence	
☐	Create a Microsoft Active Directory service account for the BEMS software.
BEMS: Skype for Business	
☐	Verify that your environment is running one of the following: • A version of BlackBerry UEM that supports BEMS. For instructions on installing or upgrading BlackBerry UEM, see the BlackBerry UEM Installation and Upgrade content. • A BlackBerry Dynamics server that supports BEMS. **Important**: The BlackBerry Dynamics server must already be installed and operational before installing BEMS.
☐	Verify that you have a supported instant messaging server.
☐	Make sure that the BEMS service account is a local administrator on the server.
☐	Make sure that the BEMS service account has "Log on as a service" permission.

Complete	Requirement
☐	Verify that the servers that host and access the BEMS Dashboard have a supported browser installed.
☐	Make sure that the server's date and time are set correctly.
☐	Make sure that the server is joined to the domain.
☐	Verify that the servers are running an operating system that supports the Connect service before you install or upgrade.
☐	If your environment runs Skype for Business on-premises for Presence and plan to configure the Connect service as trusted by Skype for Business, make sure that Windows PowerShell (x86) is installed. Open “Windows PowerShell (x86)” and run the following command to enable execution of remote signed scripts: `Set-ExecutionPolicy -Scope CurrentUser RemoteSigned`
☐	If your environment includes Skype for Business on-premises and plan to configure the Connect service as trusted by Skype for Business, create a Trusted Application Pool, trusted application, and trusted application endpoint for BEMS in the Microsoft Lync Shell Console. **Note:** The user creating the Trusted Application Pool must have RTCUniversalServerAdmins and Domain Admins permissions. For more information about preparing the first server hosting BEMS, see Prepare the initial computer hosting BEMS.
☐	If your environment includes the following instant messaging server, verify the version of Microsoft .NET Framework: Skype for Business on-premises and plan to configure the Connect service as non-trusted by Skype for Business. For more information, see Preparing the computer that hosts BEMS for use with Skype for Business.
☐	If your environment runs Skype for Business on-premises for Presence and plan to configure the Connect service as trusted by Skype for Business, make sure that the required Microsoft Unified Communications Managed API is installed. For more information, see Preparing the computer that hosts BEMS for use with Skype for Business.
☐	If your environment runs Skype for Business on-premises for Presence and plan to configure the Connect service as trusted by Skype for Business, request and install an SSL certificate on BEMS.For more information, see SSL certificate requirements for Skype for Business.
☐	Disable all antivirus programs and backup software before you install or upgrade the BEMS software.

Complete	Requirement
☐	Verify that you have installed JRE 8 on the servers where you will install BEMS and that you have an environment variable that points to its location. For instructions, see Configure the Java Runtime Environment. For information about the supported JRE versions, see the BEMS Compatibility Matrix.
BEMS - Cisco Unified Communications Manager and Cisco IM and Presence	
☐	Verify that your environment is running one of the following: • A version of BlackBerry UEM that supports BEMS. For instructions on installing or upgrading BlackBerry UEM, see the BlackBerry UEM Installation and Upgrade content. • A BlackBerry Dynamics server that supports BEMS. **Important**: The BlackBerry Dynamics server must already be installed and operational before installing BEMS.
☐	Make sure that the BEMS service account is a local administrator on the server.
☐	Make sure that the BEMS service account has Logon As a Service permission.
☐	Make sure that the server's date and time are correctly set.
☐	Make sure that the server is joined to the domain.
☐	Disable all antivirus programs and backup software before you install or upgrade the BEMS software.
☐	Verify that you have installed JRE 8 on the servers where you will install BEMS and that you have an environment variable that points to its location. For instructions, see Configure the Java Runtime Environment. For information about the supported JRE versions, see the BEMS Compatibility Matrix.
Database	
☐	Verify your environment is running a supported database server.

<table>
<tr><th>Complete</th><th>Requirement</th></tr>
<tr><td>☐</td><td>
Depending on the configuration of your environment (for example, all BEMS services on one server or on separate servers), you might need to create one or more SQL Server databases.

The following table is an example of a small deployment that has all of the BEMS services installed on one server. For an example of a small deployment that has all of the BEMS services installed one server, see Example of a small BEMS deployment.
<table>
<tr><th>Services</th><th>Databases</th></tr>
<tr><td>All BEMS services on one server</td><td>• Create a database for the BlackBerry Push Notifications service and call it "BEMS_Core", if you haven't already created it.
• Create a database for the Connect service and call it "BEMS_Connect."

Note: If this is the first server in the BEMS cluster, create the database. If this is an additional server for the same BEMS cluster, then a new database is not required. Record the existing database name for the BEMS-Connect cluster.</td></tr>
</table>
The following table is an example of a large deployment that has the BEMS services installed on separate servers. For an example of a large deployment that has the BEMS services installed on separate servers, see Example of a large BEMS deployment.
<table>
<tr><th>Services</th><th>Databases</th></tr>
<tr><td>Push notifications service (Mail) and Presence service on one server</td><td>If you already created the "BEMS_Core1" database, no additional database is required.</td></tr>
<tr><td>Connect service and Presence service on one server</td><td>Create two databases. Call one "BEMS_Core3" and "BEMS_Connect."

The Presence service does not require a separate database when it is installed with a service that uses a database.</td></tr>
<tr><td>Connect service only on one server</td><td>Create two databases. Call one "BEMS_Core3" and call one "BEMS_Connect."</td></tr>
<tr><td>Presence service only on one server</td><td>Create a database and call it "BEMS_Core2."

The Presence service requires access to a database when it is installed as a separate cluster.</td></tr>
</table>
</td></tr>
<tr><td>☐</td><td>Make sure that the BEMS service account has db_owner permission to the database. For more information, visit support.blackberry.com/community to read article 42661.</td></tr>
</table>

BlackBerry Docs

The following requirements apply when you need to configure servers to support BEMS with the BlackBerry Docs service in your organization.

Complete	Requirement
Registration	
☐	Request the BlackBerry Work app from the Marketplace for Enterprise Software portal.
☐	Log in to https://account.good.com/#/a/organization//entitlements and confirm that you have the appropriate entitlements. For more information about entitlements, see "Configure BlackBerry Work connection settings" in the BlackBerry Work administration content.
Network	

☐	Verify that the following ports are open for BEMS:
	Inbound TCP ports
	• 8443 from the BlackBerry Proxy or Good Proxy server
	Outbound TCP ports
	• 80 or 443 to Microsoft SharePoint server
	• 80 or 443 to Microsoft Office Web Apps or Office Online Server
	• 17080 or 17433 to the BlackBerry Proxy or Good Proxy server
	• 1433 to the SQL Server (default)
	• 445, 139 to CIFS share
	• 389 or 636 to LDAP
	• In a SharePoint Online environment, 443 to the following:
	  • login.microsoftonline.com
	  • *.sharepoint.com
	• In an Azure Information Protection environment, 443 to the following:
	  • login.microsoftonline.com
	  • graph.microsoft.com
	  • *.aadrm.com
	• In a Box environment, 443 to *.box.com
	Outbound UDP ports
	• 137–138 to CIFS share

☐	If BEMS requires a proxy server for external access, record the following information: • Proxy server make and model: _____ • Authentication method: _____
☐	If your environment is configured for a specific version of SMB or CIFS protocol to access a File Share, make sure that BEMS is installed on a compatible Microsoft Windows operating system. Refer to your Microsoft documentation for more information on compatibility.

Complete	Requirement
Microsoft Active Directory	
☐	Create a Microsoft Active Directory service account for the BEMS software. For example, BEMSAdmin. For password considerations, see Creating a Microsoft Active Directory account for the BEMS service account.
Microsoft .NET Framework	
☐	Verify the version of Microsoft .NET Framework. For more information, see Preparing the computer that hosts BEMS for use with Skype for Business.
BEMS	
☐	Verify that your environment is running one of the following: • A version of BlackBerry UEM that supports BEMS. For instructions on installing or upgrading BlackBerry UEM, see the BlackBerry UEM Installation and Upgrade content. • A BlackBerry Dynamics that supports BEMS. **Important**: The BlackBerry Dynamics server must already be installed and operational before installing BEMS.
☐	Verify that the server hosting BEMS is running an operating system that supports BEMS. For information about the supported operating systems, see the BEMS Compatibility Matrix.
☐	Verify that you have the required hardware to host BEMS. For more information about hardware requirements, see one of the following: • In a BlackBerry UEM environment, see BlackBerry UEM Planning content. • In a Good Control environment, see the Good Secure Enterprise Suite Planning content. If you configure your environment for disaster recovery, see the Disaster recovery content.
☐	Verify that the servers that host and access the BEMS Dashboard have a supported browser installed.
☐	Make sure that the server's time and date are set correctly.
☐	Make sure that the server is joined to the domain.
☐	Verify that the environment is running a supported version of Microsoft SharePoint or Box support. For information about supported Microsoft SharePoint versions, see the BEMS Compatibility Matrix.
☐	If you are using resource based Kerberos constrained delegation or Kerberos constrained delegation (KCD), make sure that the BEMS service account is a local administrator on the server.

<table>
<tr><th>Complete</th><th>Requirement</th></tr>
<tr><td>☐</td><td>Make sure that the BEMS service account has "Log on as a service" permission.</td></tr>
<tr><td>☐</td><td>Make sure that the Windows Firewall is disabled.</td></tr>
<tr><td>☐</td><td>Disable all antivirus programs and backup software before you install or upgrade the BEMS software.</td></tr>
<tr><td>☐</td><td>Verify that you have installed JRE 8 on the servers where you will install BEMS and that you have an environment variable that points to its location. For instructions, see Configure the Java Runtime Environment. For information about the supported JRE versions, see the BEMS Compatibility Matrix.</td></tr>
<tr><td colspan="2">Database</td></tr>
<tr><td>☐</td><td>Verify your environment is running a supported database server.</td></tr>
<tr><td>☐</td><td>Depending on the configuration of your environment (for example, all BEMS services on one server or on separate servers), you might need to create one or more SQL Server databases.

The following table is an example of a small deployment that has all of the BEMS services installed on one server. For an example of a small deployment that has all of the BEMS services installed on one server, see Example of a small BEMS deployment.
<table>
<tr><th>Services</th><th>Required databases</th></tr>
<tr><td>All BEMS services on one server</td><td>Create a database for the Docs service and call it "BEMS_Docs."

Note: If this is the first server in the BEMS cluster, create the database. If this is an additional server for the same BEMS cluster, then a new database is not required. Record the existing database name for the BEMS_Docs cluster.</td></tr>
</table>
The following table is an example of a large deployment that has all of the BEMS services installed on separate servers. For an example of a large deployment that has all of the BEMS services installed separate servers, see Example of a large BEMS deployment.
<table>
<tr><th>Services</th><th>Required databases</th></tr>
<tr><td>Docs service only on one server</td><td>Create two databases. Call one "BEMS_Core4" and call one "BEMS_Docs."</td></tr>
</table></td></tr>
<tr><td>☐</td><td>Make sure the BEMS service account has db_owner permissions to the database. For more information, visit support.blackberry.com/community to read article 42661.</td></tr>
</table>

Installation and upgrade

Supported installation and upgrade paths

To upgrade BEMS, you can use the following installation and upgrade paths.

Note: When you upgrade from an earlier version of BEMS, you must complete the upgrade precheck.

You can upgrade BEMS 3.4 and later to BEMS 3.6 using the setup application on the computer that hosts the previous version of BEMS. For more information about supported upgrade paths, visit support.blackberry.com/community to read article 53472.

If you have multiple instances of BEMS in your environment, you must complete this task on each computer that hosts an instance of BEMS.

Best practices: Preparing to upgrade

When you upgrade from an earlier version of BEMS, consider the following guidelines:

- Administrators must provide their Microsoft Active Directory user credentials to log in to the BEMS Dashboard during the upgrade.
- If you are upgrading multiple instances in a cluster, you must upgrade each computer that hosts an instance of BEMS.
- If multiple BEMS instances point to a shared (common) database, new features are not available until all instances are upgraded. Running in a mixed-version environment for an extended period is not recommended.
- Special characters, for example semicolon (;), at sign (@), and slash mark (/), are not supported for the BEMS service account.

Steps to install BEMS

For a new installation of BEMS, perform the following actions:

Step	Action
1	Verify the prerequisites.
2	Complete the preinstallation tasks.
3	Install the BEMS software.

BEMS setup application modes

When you have installed a BEMS instance in your environment and you run the setup application, the following three options are available: Modify, Repair, and Uninstall.

- **Modify**: Select this option to makes changes to your environment such add or remove BEMS services (for example, BEMS-Presence or BEMS-Connect) or change the instant messaging platform in your environment. For more information on how to use the Modify option, see the appropriate content below:
  - To remove one or more BEMS services, visit support.blackberry.com/community to read article 82381.
  - To change the instant messaging service, see 'Steps to upgrade BEMS and change the instant messaging service'.
- **Repair**: Select this option to make changes to the BEMS instance such as move the BEMS database to a new Microsoft SQL Server, change service account credentials and log file locations, and rebuild the BEMS jetty keystore if it is missing. **Note:** This option does not resolve issues that might be encountered such as resetting configuration files. For more information on how to use the Repair option, see the appropriate content below:
  - To move the BEMS databases to a new SQL Server instance, visit support.blackberry.com/community to read article 45396.
  - To change the BEMS service account and account password, visit support.blackberry.com/community to read article 58463.
  - To change the log file location, visit support.blackberry.com/community to read article 42316.
  - To rebuild the jetty keystore, visit support.blackberry.com/community to read article 57959.
- **Uninstall**: Select this option to remove the BEMS software from the computer that hosts the BEMS instance.

Steps to upgrade BEMS

Before you upgrade BEMS, make sure that the BEMS debug logging level is not set to ALL. If the logging level is set to ALL, the upgrade or repair of the BEMS instance fails. For more information, visit http://support.blackberry.com/community to read article 42408.

When you upgrade BEMS to the latest version, you perform the following actions:

Step	Action
1	Review the best practices for preparing to upgrade BEMS.
2	Verify the prerequisites.
3	Upgrade the BEMS software.

Steps to upgrade BEMS and change to an alternate JRE

When you upgrade BEMS and change from Oracle JRE8 to an alternate JRE (for example, Azul Systems or Zulu), you perform the following actions. For more information about switching to an alternate JRE, visit http://support.blackberry.com/community to read article 57053.

Before you upgrade BEMS, make sure that the BEMS debug logging level is not set to ALL. If the logging level is set to ALL, the upgrade or repair of the BEMS instance fails. For more information, visit http://support.blackberry.com/community to read article 42408.

If you have multiple BEMS instances in your environment, repeat these steps on each instance.

Step	Action
1	Download and install a supported OpenJDK.
2	Configure the Java Runtime Environment to use the OpenJDK.
3	On the computer hosting the BEMS instance, stop the following BEMS services. For example, • Good Technology Connect • Good Technology Presence • Good Technology Common Services • Good Technology .NET Services Manager
4	Optionally, uninstall the Oracle JRE8. Optionally, verify the JAVA version using the command prompt. In the command prompt, type `java -version`. Press **Enter**.
5	Import any custom certificates into the new lib\security\cacerts keystore. For instructions, see "Importing CA certificates for BEMS" in the Configuring BEMS-Core content.
6	Start the Good Technology Common Services.
7	Upgrade the BEMS instance.

Steps to install BEMS instances into a cluster

When you add multiple BEMS instances to an existing BEMS instance, you create a cluster of BEMS instances.

Note: When you install additional BEMS instances, make sure that you enter the existing database servers and database names in the appropriate database screens.

Step	Action
1	BEMS is installed and configured in the environment.
2	Verify the prerequisites on each additional BEMS instance.
3	Complete the preinstallation tasks on each additional BEMS instance.

Step	Action
4	Install the BEMS software.

Prerequisites: Installing and configuring BEMS

Successful installation of BEMS requires that a supporting infrastructure of necessary hardware and software is installed. These prerequisites include:

- Core requirements
- BlackBerry Push Notifications service (PNS) requirements
- BlackBerry Connect requirements
- BlackBerry Presence requirements
- BlackBerry Docs requirements
- BlackBerry Directory Lookup requirements
- BlackBerry Follow-Me requirements
- BlackBerry Certificate Lookup requirements

Core requirements

When you configure Core, you complete the following actions:

- Verify the system and network requirements
- Configure the Java Runtime Environment (JRE)
- Set up a Windows service account for BEMS
- Verify the database requirements

System and network requirements

Verify that your environment and the servers that host BEMS meet the following system and network requirements.

Item	Requirement
Software	Verify that you have installed JRE 8 on the servers where you will install BEMS and that you have an environment variable that points to its location.
Operating system	Verify that your server is running an operating system that supports BEMS. For information about the supported operating systems, see the BEMS Compatibility Matrix.
Supported browsers	Verify that the servers that host and access the BEMS Dashboard have a supported browser installed.

Item	Requirement
Administration rights	• The user that performs the installation must have local administrative privileges on the host machine. The user that performs the installation must also have db_owner permissions to all the BEMS databases. For more information, visit support.blackberry.com/community to read article 42661. • The BEMS service account must have "Log on as a service" right. • Disable antivirus software before you install or upgrade the BEMS software. • Exclude the BEMS directory from virus scanning. • The local Windows firewall must be disabled. **Important:** A Group Firewall Policy will cause the installer to fail its prerequisite checks, even if the local firewall is disabled.

Inbound TCP Ports	The following ports must be open and ready for BEMS and not blocked by any firewall:
	• 8080 from the BlackBerry Proxy or Good Proxy server or 8082 if SSL is required for inbound BlackBerry Proxy or Good Proxy communications, respectively
	• 8443 from the BlackBerry Proxy or Good Proxy server for Push Notifications, Presence, and Docs and from Microsoft Office Web Apps or Office Online Server for Docs
	• Optionally if your environment uses Microsoft Graph, from 8443 or another configured port to the reverse proxy appliance. For information about how Microsoft Graph communicates with BEMS, see Architecture: BEMS notification flow using the Microsoft Graph API. You can complete the following:
	  • Restrict the firewall to only accept connections from Microsoft's list of IP addresses. For more information on the available Microsoft Graph Change notifications IP addresses, see https://docs.microsoft.com/en-us/microsoft-365/enterprise/additional-office365-ip-addresses-and-urls?view=o365-worldwide.
	  • Restrict the reverse proxy server to only proxy the /notificationClient URI (for example, *bems_server_name*.example.com:443/ notificationClient" ;="bems.example.com:8443/notificationClient BEMS_Pool"
	  • If the reverse proxy appliance is installed in a DMZ, make sure that port 8443 is open from the reverse proxy to each BEMS node.
	• 49555 from the on-premises Skype for Business server (for BlackBerry Connect) when the Connect service is trusted by Skype for Business
	• 49777 from Skype for Business for the Presence service
	• 61616 TCP port to and from BEMS servers in the same cluster (bidirectional)
	• 61617 TCP (SSL) to and from BEMS servers in the same cluster (bidirectional)
	Important: To support clustering, BEMS employs ActiveMQ's enterprise features. By design, network port 61616 and 61617 (SSL) are used for inter-BEMS communication. Any firewall between BEMS nodes in the same cluster should have rules allowing bi-directional communication between BEMS nodes over port 61616 and/or 61617 (SSL).

Item	Requirement

Outbound TCP Ports	Verify that the following ports are open and ready for BEMS and not blocked by any firewall:
	• 443 to BlackBerry Dynamics NOC (gdweb.good.com)
	• 443 to Microsoft Exchange, optionally to Microsoft Graph
	• 443 to Firebase Cloud Messaging (FCM) for Android Push Notification
	• 443 or 80 to Microsoft SharePoint
	• 443 to Microsoft Office Web Apps or Office Online Server
	• 5061 (for BlackBerry Connect) to the on-premises Skype for Business server configured as trusted mode
	• 17080 to the BlackBerry Proxy or Good Proxy server
	• 17433 to the BlackBerry Proxy or Good Proxy server[2]
	• 1433 to the Microsoft SQL Server (default)
	• 8443 to the Presence Web Service (CIMP server)
	• 5222 to the Presence Web Service (CIMP server)
	• 8083 to the Cisco IM and Presence Service
	• 61616 TCP port to and from BEMS servers in the same cluster (bidirectional)
	• 61617 TCP (SSL) to and from BEMS servers in the same cluster (bidirectional)
	• In a SharePoint Online environment, 433 to the following:
	  • login.microsoftonline.com
	  • *.sharepoint.com
	• In an Azure Information Protection environment, 443 to the following:
	  • login.microsoftonline.com
	  • graph.microsoft.com
	  • *.aadrm.com
	• In a Box environment, 443 to *.box.com
	Note: For installing Connect for Skype for Business, if the Skype for Business database server is using a static port then open that port. The range of ports is necessary only when the Skype for Business database server is using dynamic ports.
	Devices must be able to connect to the Apple (APNS) and cloud messaging servers to receive push notifications from BEMS. If your Wi-Fi network restricts outbound access, make sure that the proper outbound ports are open for your devices.

Item	Requirement
Internal ports	The following ports are used by BEMS: • 8080 or 8082 for use by the BlackBerry Connect service • 8101 for SSH connectivity to BEMS • 8443 for Push Notifications and Presence • 8099 for use by the .NET Component Manager • 8060 for use by the Lync Presence Provider (LPP) • 6379 for use by Lync Presence Provider (LPP) in a Skype for Business environment and BEMS-Core in a Cisco Unified Communications Manager IM and Presence environments to read and write to the Redis service database • 1001 for use by BEMS for internal process communications when Active Directory Rights Management Services (AD RMS) and Azure-IP RMS is used in the environment
TCP/IP port access to the database	1433 to the Microsoft SQL Server default
Upload BEMS statistics	For BEMS to upload the BEMS statistics to the BlackBerry Dynamics NOC, BEMS-Core must be able to access the following: • https://gwmonitor.good.com • TCP port 443 For more information, visit support.blackberry.com/community to read article 36470.
Upload log files	For BEMS to be able to upload logs, it must have access to the following: • https://login.good.com • https://gwupload.good.com • TCP port 443 For more information, visit support.blackberry.com/community to read article 36470.

[1] A plus sign (+) indicates support for service packs and updates released subsequent to the core version.

[2] BEMS requires visibility of all BlackBerry Proxy or Good Proxy servers (17080 and 17433), regardless of whether KCD is enabled or not, so that if one BlackBerry Proxy or Good Proxy fails, BEMS can communicate with the next BlackBerry Proxy or Good Proxy in the cluster for authentication tokens, etc.

Setting up a Windows service account for BEMS

For the required service account, "BEMSAdmin" is recommended. You can use the same Windows service account to install all of the BEMS service modules. For example, bemsadmin@example.com. Make sure the service account has the appropriate administrative privileges for all the BEMS service modules that you plan to install and configure. Permissions for individual service modules may not require the same privilege level as others.

Important: If you use the same service account for the Connect and Presence services, you must give the service account the RTCUniversalReadOnlyAdmins privilege.

Creating a Microsoft Active Directory account for the BEMS service account

Note: "Read Only Domain Controllers" are a feature of the Microsoft Active Directory software. Read Only Domain Controllers Microsoft Active Directory servers are not supported for BEMS. BEMS supports only writable domain controllers.

Set the following attributes for the BEMS service account:

- The account for the Connect and Presence services must be in the same Active Directory domain as the BEMS server. For more information, visit support.blackberry.com/community to read article 63703.
- This service account should be a member of local administrator group on the BEMS host machine.
- The account name (UID, distinct from the account password) must be strictly alphanumeric; no special characters are allowed with the exception of: underscore (_), hyphen (-), and period (.). For example, BEMSAdmin.
- Account Password (distinct from the account name above) must not contain these characters: semicolon (;), at sign (@), slash mark (/), caret (^), and double-quotes (").
- Password Expires option must be set to Never for this account.

Change the BEMS service account password

1. Log on to the BEMS server using the updated password.
2. Open the Services window.
3. For the Good Technology Common Services,
   - If the Log On As services is Local System, no action is required.
   - If the Log On As services is service account, update the password and click **Apply**. Restart the services.
4. For the Good Technology Connect service and Good Technology Presence service,
   - If the Log On As services is Local System, no action is required.
   - If the Log On As services is service account, update the password and click **Apply**. Restart both services.
5. Log on to the BEMS dashboard.
6. Under **BlackBerry Services Configuration**, click **Mail > Microsoft Exchange**. If the **Use Windows Integrated Authentication** checkbox is clear, and the same service account is used, update the password, run a test, and then save the configuration.
7. If the Good Technology Connect and Good Technology Presence services use the same service account, update that password and save the configuration.

Configure permissions for the service account

A service account is a Windows account that runs the services for BEMS. The BEMS service account must be a member of the local Administrators group on the computer that you install BEMS on, and it must have the Log on as a service permission. The service account must also have permission to access the Microsoft SQL Server.

1. On the taskbar, click **Start > Administrative Tools > Computer Management**.
2. In the left pane, expand **Local Users and Groups**.
3. Navigate to the **Groups** folder.
4. In the right pane, double-click **Administrators**.
5. Click **Add**.
6. In the **Enter the object names to select** field, type the name of the service account (for example, BESAdmin).
7. Click **OK**.
8. Click **Apply**.
9. Click **OK**.

10. On the taskbar, click **Start > Administrative Tools > Local Security Policy**.
11. In the left pane, expand **Local policies**.
12. Click **User Rights Assignment**.
13. Configure the **Log on as a service** permission for the service account.

Database requirements

Make sure that your environment is running a supported version of database server. For more information about the supported databases, see the BEMS Compatibility Matrix

Configure the Java Runtime Environment

JRE 8 is required for BEMS support of intranet applications and other e-business solutions that are the foundation of corporate computing. After installing the JRE, the `JAVA_HOME` system environment variable must be set.

Important: It is recommended to disable the auto-updates to the Java Runtime Environment to avoid possible disruption of the BEMS notification function. For instructions on how to upgrade the Java version, visit support.blackberry.com/community to read article 48312.

1. On the computer that hosts BEMS, right-click **This PC** > **Properties**.
2. Click **Advanced system settings**.
3. Click the **Advanced** tab.
4. Click **Environment Variables**.
5. In the **System variables** list, complete one of the following tasks:
   - If **JAVA_HOME** does not exist, create the variable. click **New**. In the **Variable name** field, type `JAVA_HOME`.
   - If the **JAVA_HOME** variable exists, click **Edit**.
6. In the **Variable value** field, type the full path to the Java install folder for the 64-bit JRE. For example, type `C:\Program Files\Java\jre1.8.0_<version>` or `C:\Program Files\Zulu\zulu-8-jre`

   If you use an OpenJDK version and include the direct path to the java.exe file, the BEMS installer returns the error message: **Could not find a valid Java virtual machine to load. You may need to reinstall a supported java virtual machine**.
7. Click **OK**.
8. In the **System variables** section, locate the **Path** variable. Click **Edit**.
9. In the **Variable value** field, append the *JAVA_HOME* variable, separated by a semi-colon. For example, add `;%JAVA_HOME%\bin`
10. Click **OK**. Click **OK** again.

Prerequisites: Connect for Skype for Business

Note: The prerequisites discussed here do not apply to Cisco Unified Communications Manager for IM and Presence environments, when Jabber is selected during the BEMS server installation for use with the Connect service.

If your environment uses multiple Skype for Business on-premises servers using trusted application mode or non-trusted application mode, have the Skype for Business servers load balanced with a load balance server. For more information about load balancing requirements, visit https://docs.microsoft.com/en-us/skypeforbusiness/plan-your-deployment/network-requirements/load-balancing.

If you configure Connect for Skype for Business with the Connect service configured as trusted by Skype for Business, complete the following pre-requisites:

- Preparing the computer that hosts BEMS for use with Skype for Business
- BlackBerry Connect service database requirements
- Prepare the Skype for Business Topology for Connect
- SSL certificate requirements for Skype for Business

If you configure Connect for Skype for Business with the Connect service configured as non-trusted by Skype for Business, complete the following pre-requisites:

- Preparing the computer that hosts BEMS for use with Skype for Business
- BlackBerry Connect service database requirements

Preparing the computer that hosts BEMS for use with Skype for Business

If you plan to install BEMS for use with Skype for Business, you must verify that the computer that you install BEMS on meets specific requirements.

Note: All instant messaging server platforms, require the Connect service to be installed on a computer that runs Microsoft Windows Server 2012, Windows Server 2016, Windows Server 2019, or Windows Server 2022.

Turn off antivirus software for computers running BEMS with BlackBerry Connect and BlackBerry Presence.

Before you install BEMS, you must perform the following actions in the order that they are listed. Complete these tasks on each computer that hosts the Connect service.

1. Install and enable a command-line shell and scripting tool.
   - On a computer that is running Windows Server 2016, Windows Server 2019, or Windows Server 2022, Windows PowerShell is enabled by default. Open Windows PowerShell and run the following script:

     ```
     Set-ExecutionPolicy -Scope CurrentUser RemoteSigned
     ```
   - On a computer that is running Windows Server 2012, if required, use the Windows Server Manager to add Windows PowerShell 3.0 as a feature. When the installation prompts you to restart the computer, click **Yes**.

     Open Windows PowerShell and run the following script:`Set-ExecutionPolicy -Scope CurrentUser RemoteSigned`
2. Install and enable Microsoft .NET Framework 4.6 or later. For more information about .Net Framework system requirements, visit https://docs.microsoft.com/en-us/dotnet/framework/get-started/system-requirements.
   - On a computer that is running Windows Server 2016, Windows Server 2019, or Windows Server 2022, no action is required. Microsoft .NET Framework is installed and enabled by default.
   - On a computer that is running Windows Server 2012, use the Windows Server Manager to add Microsoft .NET Framework as a feature. When the installation prompts you to restart the computer, click **Yes**.
3. Complete one of the following tasks using the Windows Server Manager:
   - If you install BEMS on a computer that is running Windows Server 2016, Windows Server 2019, or Windows Server 2022, no action is required.
   - If you install BEMS on a computer that is running Windows Server 2012, install **Media Foundation**. When the installation prompts you to restart the computer, click **Yes**.
4. Download and install Microsoft Unified Communications Managed API.

   Note: Consult your vendor documentation to determine if the Microsoft Unified Communications Managed API version is supported by your operating system.

   If you use Skype for Business 2015 or Skype for Business 2019, download Microsoft Unified Communications Managed API 5.0 Runtime (UcmaRuntimeSetup.exe). To download the file, visit www.microsoft.com/download and search for ID=47344.

Note: UCMA 6.0 is not supported.

5. Run **OCSCore.msi**. This file is included with the Microsoft Unified Communications Managed API and located in a hidden folder at `<drive>:\ProgramData\Microsoft\<instant messaging server type>\Deployment\cache\<version>\Setup\`
6. If you enable persistent chat in a Skype for Business 2015 environment, download and install Microsoft Visual C++2012 x64 Minimum Runtime – 11.0.50727. To download the file, click here.

   Note: Persistent chat is not supported in a Skype for Business 2019 environment. For more information, see https://docs.microsoft.com/en-us/skypeforbusiness/deprecated.
7. Install the latest service pack and critical Windows updates on your computer.

BlackBerry Connect service database requirements

You must create a blank SQL database for the Connect service. The recommended name for this database is BEMS_Connect .

If you installed the Connect service on a separate computer, you must create two SQL databases and call them "BEMS_Core3" and "BEMS_Connect".

During installation, you are prompted to specify the database server and Microsoft SQL Server instance. When you enter this information, the BEMS installation files automatically create the schema required by the Connect service.

Note: If your environment includes a single BEMS cluster, only one SQL database is required for all computers hosting the BlackBerry Connect

Preparing the Skype for Business topology for BEMS

The Connect service and Lync Presence Provider (LPP) are Microsoft Lync trusted-UCMA applications. You must be a member of the RTCUniversalServerAdmins and Domain Admins security groups to provision and publish new applications in the Skype for Business Topology. If you have a designated Skype for Business administrator within your organization, that person should perform all subsequent preparation steps for this procedure.

To provision the computer hosting the Connect and Presence services as trust application servers with the Skype for Business, you must use the Skype for Business Management Shell to complete the following tasks:

1. Create a trusted application pool as a virtual container for one or more computers hosting the BEMS-Connect service and the BEMS-Presence service.
2. Designate trusted applications for the use of the BEMS computer.
3. Create a trusted-computer entry for every BEMS in the environment.
4. Create one or more virtual trusted application endpoints for the Presence service.
5. Publish these changes to the Skype for Business topology.

A trusted application pool is a virtual pool or container of one or more trusted application servers, (for example, the Connect service and the Presence service). The trusted application cmdlets define parameters for the services available in the trusted application servers that are associated with the trusted application pool, (for example, the application identifier for Connect service and the Presence service and the listening ports used by these services). The trusted application pool doesn't provide load balancing services for the Connect and Presence services. It only provides configuration and registration information to the Skype for Business to allow the messaging servers to route incoming chat requests or presence status updates to the mobile users being managed by each Connect and Presence service. A BlackBerry Connect app user cannot be represented by more than one BEMS-Connect service at any time. Any type of load balancing or user endpoint distribution is managed by the Connect service directly. For more information about sizing requirements, see the BEMS Performance Calculator.

A trusted application endpoint represents a virtual user to allow the Presence service to subscribe to SIP-enabled users to receive presence availability updates and make this information available to mobile users (for example,

BlackBerry Work users). One or more trusted application endpoints must be created for each Presence service on the Skype for Business to process subscriptions. "Trusted application endpoint" only refers to the virtual user used by the Presence service to make the subscription requests. The endpoint remains on the computer hosting the BEMS-Presence service. The Presence service only communicates with the Front End Pool using port 5061. When a subscription is made to a SIP-enabled user to receive availability updates, the Skype for Business Front End Pool sends the user's updated presence status on port 49777 to the Presence service. The number of subscriptions handled by each Presence service and each trusted application endpoint used by the Presence service is managed by the Presence service. For more information about creating trusted application endpoints, see "Manually configure the Presence service for multiple application endpoints" in the Presence Configuration content.

Important: If you change the instant messaging server from Skype for Business, you must remove the existing provisioning of BEMS as a trusted application and trusted application pool and then establish trust with the Create a trusted application pool by preparing the initial computer hosting Skype for Business server. For steps on changing the instant messaging service, see Steps to upgrade BEMS and change the instant messaging service.

You must complete the application provisioning process described in the following instructions:

- Preparing the initial computer hosting BEMS
- Preparing additional computers hosting BEMS. If you installed the BEMS services on separate computers, you must complete this step for each computer.

After updating the topology, the administrator must delegate RTCUniversalReadOnlyAdmins permission to the BEMS service account for the BEMS Dashboard to access the provisioning information during the BEMS configuration process.

Prepare the initial computer hosting BEMS

When you create a trusted application pool for the installation of BEMS, you also create the trusted-computer entry. Subsequent installations of BEMS machines do not require a new trusted application pool or designated trusted applications because they are added to the existing trusted application pool.

Before you begin: Verify that the account that you use to complete this task is a member of the RTCUniversalServerAdmins group.

1. Log in to the computer that hosts the Skype for Business.
2. Open the **Management Shell**.
3. On the computer that hosts Skype for Business, create the trusted application pool.
   a) To obtain the SiteID of your Skype for Business, type `Get-CsSite`. Press **Enter**. Record the SiteID.
   b) To display the Registrar service value for a selected site, type `Get-CsSite <SiteID> | Select-Object -ExpandProperty Services`. Press **Enter**. Record the Registrar service value.
   c) To configure the trusted application entry for the newly created trusted application pool for BEMS, type `New-CsTrustedApplicationPool -Force -Identity <YourPoolFQDN> -Registrar <registrar> -RequiresReplication $false -Site <SiteID> -ComputerFQDN <BEMSFQDN>`. Press **Enter**.
      - Where <*YourPoolFQDN*> is the desired FQDN of the virtual Application pool of the BEMS instances.
      - Where <*SiteID*> is the SiteID that was recorded in step 3a.
      - Where <*registrar*> is the value recorded in step 3b.
      - Where <*BEMSFQDN*> is the FQDN of computer hosting BEMS.

      For example,
      ```
      New-CsTrustedApplicationPool -Force -Identity
      BEMSAppPool.mycompany.com -Registrar registrar.mycompany.com -
      RequiresReplication $false -Site 1 -ComputerFQDN BEMSHost.mycompany.com
      ```

d) To create a trusted application entry, type `New-CsTrustedApplication -Force -ApplicationId <appid_connect> -TrustedApplicationPoolFqdn <YourPoolFQDN> -Port 49555`. Press **Enter**.

Where <*appid_connect*> is the desired application ID of the BEMS Connect service.

For example, `New-CsTrustedApplication -Force -ApplicationId appid_connect -TrustedApplicationPoolFqdn BEMSAppPool.mycompany.com -Port 49555`

e) If you deploy the Presence service, create a second application entry. Type `New-CsTrustedApplication -Force -ApplicationId <appid_presence> -TrustedApplicationPoolFqdn <YourPoolFQDN> -Port 49777`. Press **Enter**.

Where <*appid_presence*> is the desired application ID of the BEMS Presence service.

For example, `New-CsTrustedApplication -Force -ApplicationId appid_presence -TrustedApplicationPoolFqdn BEMSAppPool.mycompany.com -Port 49777`

f) If you deploy the Presence service, create an application endpoint. Type `New-CsTrustedApplicationEndpoint -ApplicationId <appid_presence> -TrustedApplicationPoolFqdn <YourPoolFQDN> -SipAddress "sip:presence_<BEMSFQDN>@<SIPDomain>"`.

For example, `New-CsTrustedApplicationEndpoint -ApplicationId appid_presence -TrustedApplicationPoolFqdn BEMSAppPool.mycompany.com -SipAddress "sip:presence_BEMSHost.mycompany.com@mycompany.com"`

g) To publish the change to the Skype for Business environment, type `Enable-CsTopology`. Press **Enter**.

After you finish: If you are installing multiple BEMS servers, see Prepare additional computers hosting BEMS.

Prepare additional computers hosting BEMS

Before you begin:

- Verify that a BEMS server is installed in your environment, and a trusted application pool and trusted computer entry is created according to the instructions in Prepare the initial computer hosting BEMS.
- Verify that the account that you use to complete this task is a member of the RTCUniversalServerAdmins group.

1. Log in to the computer that hosts the Skype for Business using an account with RTCUniversalServerAdmins group permissions.
2. Open the **Management Shell**.
3. On the computer that hosts Skype for Business, create the trusted computer for the BEMS trusted application pool.
   a) To add the trusted computer for the BEMS trusted application pool, type `New-CsTrustedApplicationComputer -Identity <BEMSFQDN> -Pool <YourPoolFQDN>`.
   - Where <*BEMSFQDN*> is the FQDN of computer hosting BEMS.
   - Where <*name of BEMS pool previously created*> is the name of the BEMS pool in step 3c of Prepare the initial computer hosting BEMS

   For example: `New-CsTrustedApplicationComputer -Identity BEMSHost2.mycompany.com -Pool BEMSAppPool.mycompany.com`
4. If the computer hosting BEMS runs the BEMS Presence service, create an application endpoint. Type `New-CsTrustedApplicationEndpoint -ApplicationId <appid_presence> -TrustedApplicationPoolFqdn <YourPoolFQDN> -SipAddress "sip:presence_<BEMSFQDN>@<SIPDomain>"`. Press **Enter**.

   Where <*appid_presence*> is the desired application ID of the BEMS Presence service.

For example: `New-CsTrustedApplicationEndpoint -ApplicationId appid_presence -TrustedApplicationPoolFqdn BEMSAppPool.mycompany.com -SipAddress "sip:presence_BEMSHost2.mycompany.com@mycompany.com"`

5. To publish the change to Skype for Business environment, type `Enable-CsTopology`. Press **Enter**.

Creating an additional trusted application pool

One BlackBerry Connect instance can be associated with only one Trusted Application Pool. In a high availability or disaster recovery scenario, it is recommended that you create an additional trusted application pool in your Front-End high availability and disaster recovery pool for your Connect high availability and disastery recovery instances.

The steps for creating an additional trusted application pool are the same as creating your first trusted application pool for Connect with the exception that trusted application pool names must be unique. Therefore, if you named your first trusted application pool "pool1_bems.example.com", then your second trusted application pool name must be different. For example, "pool2_bems.example.com".

Removing provisioning of the BEMS as a trusted application and trusted application pool

You can use Windows PowerShell to remove the provisioning of the BEMS as a trusted application software and trusted application pool before you remove the Connect service and Presence service from the BEMS instances in your organization's network.

When you remove provisioning of BEMS as a trusted application, the provisioning record is removed from Microsoft Active Directory. When the provisioning record is removed from Microsoft Active Directory, BEMS remains running, but the communication to the Microsoft Lync Server stops.

Remove provisioning of the BEMS as a trusted application and trusted application pool

If your environment is running Skype for Business, you must remove provisioning of the BEMS as a trusted application and trusted application pool using the Microsoft Lync Server Management Shell that you used to create it.

1. Log in to the computer that hosts Skype for Business using an account with RTCUniversalServerAdmins group rights.
2. Open a Management Shell window and complete the following steps:
   a) To display the Trusted Application Pool that the computer is a part of, type `Get-CsTrustedApplicationComputer -Identity <FQDN_of_the_bems_host>`. Press **Enter**. Record the Pool name.
   b) To display all the computers in the Pool name recorded in step 2a, type `Get-CsTrustedApplicationPool -pool <FQDN_of_the_pool_from_step_a>.` Record if more than one FQDN entry is listed.
   c) To display additional information about the above Trusted Application Pool, type `Get-CsTrustedApplicationPool -PoolFqdn <FQDN_of_the_pool_from_step_a>`. Press **Enter**.
   d) To remove one BEMS instance from the trusted application pool when you have more than one BEMS instance in your organization’s environment, type `Remove-CsTrustedApplicationComputer -Identity <FQDN_of_the_bems_host>.` Press **Enter**.
   e) To remove all BEMS instances from the Trusted Application Pool and remove the pool itself, type `Remove-CsTrustedApplicationPool -Identity <FQDN_of_the_pool_from_step_2a>`.
   f) To publish the change to the Skype for Business environment, type `Enable-CsTopology`. Press **Enter**.
   g) To verify that the trusted application pool is removed, type `Get-CsTrustedApplicationComputer -Identity <FQDN_of_the_bems_host>`.

SSL certificate requirements for Skype for Business

If your enterprise doesn't already have one, or one designated for use by BEMS, you must obtain and install a digital certificate.

Your enterprise can sign its own digital certificates, acting as its own certificate authority (CA), or you can submit a certificate request to a well-known, third-party CA. Although you can preinstall the root authority for your own CA on each user's device, it makes sense to get an independent CA-validated certificate.

Note: In the following sections, references to SSL, CA-signed, and personal certificates refer to the digital certificate.

Mutual TLS (MTLS) certificates

Connect and Lync Presence Provider (LPP) connections to Skype for Business rely on mutual TLS (MTLS) for mutual authentication. On an MTLS connection, the server originating a message and the server receiving it exchange certificates from a mutually trusted CA. The certificates prove the identity of each server to the other.

In Skype for Business deployments, certificates issued by the enterprise CA that are valid and not revoked by the issuing CA are automatically considered valid by all internal clients and servers because all members of a Microsoft Active Directory domain trust the Enterprise CA in that domain. In federated scenarios, the issuing CA must be trusted by both federated partners. Each partner can use a different CA, if desired, so long as that CA is also trusted by the other partner. This trust is most easily accomplished by the Edge Servers having the partner's root CA certificate in their trusted root CAs, or by use of a third-party CA that is trusted by both parties.

Hence, BEMS must form a mutual trust relationship for MTLS communications supporting its network server environment. Mutual trust requires a valid SSL certificate that meets the following criteria:

- The following certificates must be stored on the computer that hosts BEMS in the Windows Certificate store. You can access the certificates using the Microsoft Management Console (MMC).
  - The private certificate issued for BEMS by a trusted CA and that is accessible using the Microsoft Management Console (MMC) in the `Console Root\Certificates <local_host_name>\Personal \Certificate` folder.
  - The BEMS computer's private certificate and the Skype for Business internal computer certificate must both be trusted by root certificates and accessible using the Microsoft Management Console (MMC) in the `Console Root\Certificate <local_host_name>\Trusted Root Certification Authorities\Certificates` folder.
  - Intermediate certificates for both the BEMS private certificate and the Skype for Business internal computer certificate and accessible using the Microsoft Management Console (MMC) in the `Console Root\Certificates <local_host_name>\Intermediate Certification Authorities \Certificates` folder.
- The Subject Name certificate property must contain the Common Name (CN) of a valid FQDN such as a trusted application pool name (for example, CN=bemsapppool.example.com). For more information about the trusted application pool name, see Prepare the initial computer hosting BEMS.
- The Subject Alternative Name (SAN) certificate property must include the FQDN for the trusted application pool and the FQDN of each BEMS instance that the certificate will be used for (for example, bemsapppool.example.com, bemsserver01.example.com, bemsserver02.example.com, bemserver03.example.com, and so forth).
- The certificate must be signed by a CA that is mutually trusted by both Skype for Business and BEMS.

Note: The account used to run BEMS must have read access to the certificate store and the private key. You can assign read rights to the private key by right-clicking on the certificate.

For more information about generating SSL certificates with subject alternative names, visit the Technet Library to see How to generate a certificate with subject alternative names (SAN).

Steps to create a CA-signed certificate for the local computer account using a CSR for BEMS

When you create a CA-signed certificate for the local computer account for BEMS that can be used on all computers hosting BEMS, you perform the following actions.

Step	Action
1	Create a CSR for the local computer account for BEMS
2	Obtain a CA-signed certificate from the CA server
3	Import the CA-signed certificate on the CSR requesting BEMS
4	Export the CA-signed certificate and private key from the Microsoft Management Console
5	Import the CA-signed certificate and private key to additional BEMS instances

Steps to create a CA-signed for the local computer account using automatic enrollment for BEMS

When you create a Personal Certificate for the local computer account for BEMS that can be used on all computers hosting BEMS, you perform the following actions.

tep	Action
1	Create a Personal Certificate for the local computer account for BEMS
2	Export the CA-signed certificate and private key from the Microsoft Management Console
3	Import the CA-signed certificate and private key to additional BEMS instances

Create a CSR for the local computer account for BEMS

If you want to use an enterprise CA to generate the SSL certificate, you must create a custom request on a computer that hosts BEMS.

1. On the computer that hosts BEMS, open the Microsoft Management Console.
2. Click **Console Root**.
3. Click **File > Add/Remove Snap-in**.
4. In the **Available snap-ins** column, click **Certificates**. Click **Add**.
5. In the **Certificates snap-in** wizard, select **Computer account**. Click **Next**.
6. On the **Select Computer** screen, select **Local computer**.

7. Click **Finish**. Click **OK**.
8. In the Microsoft Management Console, expand **Certificates (Local Computer)**.
9. Right-click **Personal**, then click **All Tasks > Advanced Operations > Create Custom Request**.
10. In the **Certificate Enrollment wizard**, click **Next**.
11. Click **Proceed without enrollment policy**. Click **Next**.
12. On the **Custom request** screen, click **Next**.
13. On the **Certificate Information** screen, click the **Details > Properties**.
14. On the **Subject** tab, in the **Subject name** section, complete the following actions:
    a) Click the **Type** drop-down list. Select **Common Name**.
    b) In the **Value** field, type a valid FQDN such as a trusted application pool name (for example, CN=bemsapppool.example.com) that was recorded in step 3c of Prepare the initial computer hosting BEMS.
    c) Click **Add**.
15. In the **Alternative name** section, add two values by completing the following actions:
    a) Click the **Type** drop-down list. Select **DNS**.
    b) In the **Value** field, type the FQDN of the trusted application pool (for example, bemsapppool.example.com).
    c) Click **Add**.
    d) In the **Value** field, type the FQDN of a BEMS instance that the certificate will be used for (for example, bemsserver01.example.com).
    e) Click **Add**.
    f) Repeat steps d and e for each BEMS instance that the certificate will be used for (for example, bemsserver02.example.com, bemserver03.example.com, and so forth).
16. Optionally, on the **General** tab, specify a friendly name for the certificate. The name of the template is often the only way to distinguish its purpose and must be unique. This is important when deploying the final name of the issued certificate, which should always match the designated service name. For more information about using friendly names for certificates in Connect and Presence, see "Using friendly names for certificates in BlackBerry Connect" in the Connect configuration content and "Using friendly names for certificates in BlackBerry Presence" in the Presence configuration content.
    a) Click the **General** tab.
    b) In the **Friendly name** field, enter a name.
17. On the **Private Key** tab, verify that the template allows the certificate to be exported with the private key.
    a) Click the **Private Key** tab.
    b) Click the **Key options** drop-down list. Select the **Make private key exportable** check box.
18. Click **Apply**.
19. Click **OK**.
20. Click **Next**.
21. Save the certificate information to your desktop with a file format of Base 60.
22. Click **Finish**.

After you finish: Obtain a CA-signed certificate from the CA server

Obtain a CA-signed certificate from the CA server

Before you begin: Verify that you have access to the CSR file that was created in Create a CSR for the local computer account for BEMS.

1. Open the CSR certificate information and copy the certificate information, including the Begin and End Certificate request lines.

2. Access the CA server and obtain the CA-signed certificate.

After you finish: Import the CA-signed certificate on the CSR requesting BEMS.

Import the CA-signed certificate on the CSR requesting BEMS

You must import the CA-signed certificate on the BEMS instance that requested the CSR to pair the public and private keys.

Before you begin: Verify that you have access to the CA-signed certificate that you obtained.

1. On the computer that hosts BEMS , in the **Microsoft Management Console**, expand **Personal**.
2. Right-click **Certificates**, then click **All Tasks > Import**.
3. Click **Next**.
4. Navigate to the signed CA-certificate that you obtained. Click **Next**.
5. Click **Next** again.
6. Click **Finish**.

After you finish: Export the CA-signed certificate and private key from the Microsoft Management Console

Create a Personal Certificate for the local computer account for BEMS

Complete this task on each computer that hosts the Presence and/or Connect service. You can create one certificate to be used for all BEMS instances.

1. On the computer that hosts BEMS, open the Microsoft Management Console.
2. Click **Console Root**.
3. Click **File > Add/Remove Snap-in**.
4. In the **Available snap-ins** column, click **Certificates**. Click **Add**.
5. In the **Certificates snap-in** wizard, select **Computer account**. Click **Next**.
6. On the **Select Computer** screen, select **Local computer**.
7. Click **Finish**. Click **OK**.
8. In the Microsoft Management Console, expand **Certificates (Local Computer)**.
9. Right-click **Personal**, then click **All Tasks > Request New Certificate**.
10. In the **Certificate Enrollment wizard**, click **Next**. Click **Next** again.
11. Select an appropriate web server template from the available templates.
    a) Click **Details** to verify that the Server Authentication is displayed in the Application Policies section.
    b) In the **Application policies** section, verify that **Server Authentication** is listed. If Server Authentication is not listed, select a different web server template. Contact your CA administrator for more information about templates.
12. Click **More information is required to enroll for this certificate. Click here to configure settings**.
13. On the **Subject** tab, in the **Subject name** section, complete the following actions:
    a) Click the **Type** drop-down list. Select **Common Name**.
    b) In the **Value** field, type a valid FQDN such as a trusted application pool name (for example, CN=bemsapppool.example.com) that was recorded in step 3c of Prepare the initial computer hosting BEMS.
    c) Click **Add**.
14. In the **Alternative name** section, add two values by completing the following actions:
    a) Click the **Type** drop-down list. Select **DNS**.
    b) In the **Value** field, type the FQDN of the trusted application pool (for example, bemsapppool.example.com).

c) Click **Add**.
d) In the **Value** field, type the FQDN of a BEMS instance that the certificate will be used for (for example, bemsserver01.example.com).
e) Click **Add**.
f) Repeat steps d and e for each BEMS instance that the certificate will be used for (for example, bemsserver02.example.com, bemserver03.example.com, and so forth).

15. Optionally, on the **General** tab, specify a friendly name for the certificate. The name of the template is often the only way to distinguish its purpose and must be unique. This is important when deploying the final name of the issued certificate, which should always match the designated service name. For more information about using friendly names for certificates in Connect and Presence, see "Using friendly names for certificates in BlackBerry Connect" in the Connect configuration content and "Using friendly names for certificates in BlackBerry Presence" in the Presence configuration content.
    a) Click the **General** tab.
    b) In the **Friendly name** field, enter a name.
16. On the **Private Key** tab, verify that the template allows the certificate to be exported with the private key.
    a) Click the **Private Key** tab.
    b) Click the **Key options** drop-down list. Select the **Make private key exportable** check box.
17. Click **Apply**.
18. Click **OK**.
19. Click **Enroll**.
20. Click **Finish**.

After you finish:

- Grant the service account read access to the certificate.
  1. Right-click the certificate, and click **All Tasks > Manage Private Keys**.
  2. On the **Security** tab, add the service account.
- Export the certificate and the private key, then import the certificate to each of the other computers that host a BEMS instance. For instructions, see Export the CA-signed certificate and private key from the Microsoft Management Console and Import the CA-signed certificate and private key to additional BEMS instances respectively.

Export the CA-signed certificate and private key from the Microsoft Management Console

Export the certificate from the Microsoft Management Console (MMC). Make sure to include the private key and save it as a .pfx file. For more information, visit docs.microsoft.com and read 'Export a Certificate with the Private Key'

Before you begin: Verify that you created a CA-signed certificate for the local computer account to use on multiple BEMS instances running the Connect and/or Presence services. For instructions on creating a CA-signed certificate using automatic enrollment, see Create a Personal Certificate for the local computer account for BEMS. For instructions on creating a CA-signed certificate using a CSR, see Create a CSR for the local computer account for BEMS.

1. On the computer that hosts BEMS, open the Microsoft Management Console.
2. Expand **Personal**.
3. Click **Certificates**.
4. Right-click the personal certificate that you created and click **All Tasks > Export**.
5. In the **Certificate Export Wizard**, select **Yes, export the private key**.
6. Click **Next**.

7. Verify that the **Include all certificates in the certification path if possible** check box is selected. Clear the other check boxes.
8. Select the appropriate security method and enter the required security information. Click **Next**.

   If you select Groups and users, make sure that you log on to the BEMS instance where the certificate will be imported as the user or member of that group.
9. Click **Browse** to specify a name for the certificate and save it to your desktop.
10. Click **Next**.
11. Click **Finish**.
12. Click **OK**.

After you finish: Import the CA-signed certificate and private key to additional BEMS instances.

Import the CA-signed certificate and private key to additional BEMS instances

Complete this task on each computer that hosts the Presence and/or Connect service and is configured to use Skype for Business. You can use one signed certificate for multiple BEMS instances. For more information about importing the certificate, visit docs.microsoft.com and read 'Import a Certificate'.

Before you begin:

- Verify that you have the access to the exported signed certificate. Instructions, see Export the CA-signed certificate and private key from the Microsoft Management Console
- If the certificate was exported and a security principal was specified, you must log in as a member of that specified group or user.
- Make sure that you have the password that is assigned to the exported certificate.

1. On the computer that hosts BEMS, open the Microsoft Management Console.
2. Expand **Personal**.
3. Right-click **Certificates**, then click **> All Tasks > Import**.
4. Click **Next**.
5. Navigate to the certificate that you want to import. Click **Next**.
6. Enter the password for the private key. Click **Next**.
7. Click **Finish**.

Presence prerequisites: Skype for Business

For Skype for Business, the Presence service has the same predeployment requirements as the Connect service. The Presence service does not require its own Microsoft SQL Server database when it is installed on a computer with the BlackBerry Push Notifications (Mail) service or on a computer with the Connect service. If you installed the Presence service on a separate computer, you must create a database. It is recommended to call the database BEMS_Core2. For more information about prerequisites, see the following: Prerequisites: Connect for Skype for Business

Note: Presence for Skype for Business on-premises using non-trusted application mode doesn't use the Good Technology Presence service. Therefore, there is no requirement to start the service, and no requirement to make sure that an MTLS certificate is issued for the Presence service to use. Presence status is provided by Good Technology Common Services service.

Prerequisites: BlackBerry Push Notifications service

BlackBerry Push Notifications service requires a database, and that you set up a Windows service account for BEMS in support of your Microsoft Exchange environment.

In general, Microsoft Exchange Web Services (EWS) push notifications are sent (or pushed) by the server to a client-side web service. Push notifications are ideally suited for tightly coupled clients like BlackBerry Work and other BEMS supported apps to which the server has reliable access. When the BlackBerry Push Notifications service is configured, Microsoft Exchange Web Services events are sent.

If you deploy BEMS in a mixed environment, where BEMS and Microsoft Exchange are not co-located, there are additional requirements and prerequisites which may apply. Consider the following scenarios:

Cloud-based BEMS with on-premise Microsoft Exchange

1. You must expose Microsoft Exchange Web Services and Autodiscover from your on-premise Microsoft Exchange to the Internet on port 443.
2. Both Basic Authentication and Windows Authentication are supported for Microsoft Exchange Web Services and Autodiscover.

On-Premise BEMS with Cloud-based Exchange

1. You must expose Microsoft Exchange Web Services and autodiscover from cloud-based Microsoft Exchange to on-premise BEMS on port 443.
2. Although both basic authentication and Windows authentication are supported by BEMS, be advised that certain cloud vendors—for instance, Microsoft Office 365 and Rackspace—only support basic authentication. Check with your specific cloud vendor for details.

On-premise BEMS with on-premise and cloud-based Microsoft Exchange

1. You must expose Microsoft Exchange Web Services and autodiscover from cloud-based Microsoft Exchange to on-premise BEMS on port 443.
2. Although both basic authentication and Windows authentication are supported by BEMS, be advised that certain cloud vendors—for instance, Microsoft Office 365 and Rackspace—only support basic authentication. Check with your specific cloud vendor for details.
3. The BEMSAdmin account must have impersonation rights on both the on-premise and Microsoft Office 365 Microsoft Exchange systems. For more information on granting application permissions, see Grant application impersonation permission to the service account.

For more information on configuring Microsoft Exchange Web Services and Autodiscover for external access, visit the Microsoft Technet Library to see the following articles:

- Configure the Autodiscover Service for Internet Access
- Configuring EWS for External Access

Grant application impersonation permission to the service account

For the BlackBerry Push Notifications service to monitor mailboxes for updates, the BlackBerry Push Notifications service account, must have impersonation permissions.

Execute the following Microsoft Exchange Management Shell command to apply Application Impersonation permissions to the service account:

- Grant application impersonation permission using Exchange Administration Center
- Grant application impersonation permission using Microsoft Exchange Management Shell

Grant application impersonation permission using Exchange Administration Center

1. Depending on your environment, sign in to one of the following consoles:

Console	Steps
Microsoft Office 365 Exchange Administration Center console	**a.** Sign in to https://portal.office.com. **b.** Click the App Launcher icon in the top left hand corner. **c.** Click **Admin**. **d.** In the **Microsoft 365 admin center** console menu, click **Show all**. **e.** In the **Admin centers** section, click **All admin centers**. **f.** Click **Exchange**.
On-premises Microsoft Exchange Administration Center web console	**a.** Open a browser open `https://<url_to_on-premises_client_access_server>/ecp` and sign in with a valid account.

2. Click **permissions**.
3. Click +.
4. Type a name and description for the role group.
5. In the **Roles** section, click +. Click **ApplicationImpersonation > add > OK**.
6. In the **Members** section, click +. Click an account to add and then click **add > OK**.

Grant application impersonation permission using Microsoft Exchange Management Shell

1. Open Microsoft Exchange Management Shell.
2. Type `New-ManagementRoleAssignment -Name:<ImpersonationAssignmentName> -Role:ApplicationImpersonation -User:<ServiceAccount>`. For example, `New-ManagementRoleAssignment -Name:BlackBerryAppImpersonation -Role:ApplicationImpersonation -User:BEMSAdmin`.

After you finish:

For more information on how to restrict Application Impersonation rights to specific users, organizational units, or security groups, visit the MSDN Library to see How to: Configure impersonation.

Microsoft Exchange Autodiscover

Ensure that your Microsoft Exchange Autodiscover is setup correctly.

The Autodiscover feature in Microsoft Exchange provides the mail client with configuration options and shares only the user's email address and password. This is useful for remote users and smartphone users, who do not want to enter advanced settings like server names and domains. It is also required for the correct functioning of features such as out of office and the offline address book in Microsoft Outlook.

Use EWSEditor to test if there are any doubts. For more information about using EWSEditor, visit support.blackberry.com/community to read article 40351.

BlackBerry Push Notifications database requirements

You must create a blank SQL database for the BlackBerry Push Notifications service. The recommended name for this database is BEMS_Core. If you install the BlackBerry Push Notifications service (Mail services

on one computer) and other services (for example, the Presence service) on another computer, call the database BEMS_Core1.

Note: Make sure the Collate property is set to CI (case insensitive). This is the default collation setting when you create a new database. If you are upgrading an existing database, verify the collation setting.

BEMS connects to the Microsoft SQL Server using TCP/IP. If your environment uses Microsoft SQL Server Express, the TCP/IP protocol is not enabled by default. For instructions on how to enable TCP/IP on Microsoft SQL Server Express, visit support.blackberry.com/community and read article 63994.

BEMS supports the use of dynamic ports when connecting to the SQL Server. Dynamic ports is the default setting for SQL Server Express installations and other more complex SQL Server installations. The SQL Server Browser service must be started for BEMS to use SQL Server dynamic ports. BEMS connects to the SQL Server Browser service over port 1434 to obtain the current dynamic port of the SQL Server instance to use. By default, the SQL Server Browser service is disabled in SQL Server Express installations.

Verify the case sensitivity of the BlackBerry Push Notifications database

Run the following SQL query: `SELECT DATABASEPROPERTYEX('dbname', 'Collation')`

Where **dbname** is the name for the BlackBerry Push Notifications database. For example, GEMSDB.

Verify the return value.

- SQL_Latin1_General_CP1_CI_AS, CI indicates that the database is case insensitive.
- SQL_Latin1_General_CP1_CS_AS, CS indicates that the database is case sensitive.

Change the BlackBerry Push Notifications case type to insensitive

To change the case sensitivity, type `alter database [dbname] collate SQL_Latin1_General_CP1_CI_AS`

During installation, you will be prompted to specify the database server and SQL instance. When this information is entered, the BEMS installer will automatically create the schema required by BlackBerry Push Notifications.

Prerequisites: Cisco Unified Communications Manager IM and Presence Service requirements for Presence

Turn off antivirus software for computers running BEMS with Connect-Presence.

Create an Application User

This application user is a logical entity that represents a third-party application that can log into Cisco Unified CM IM and Presence.

1. Log in to the Cisco Unified Communications Manager Administration console.
2. Click **User Management > Application User**.
3. Click **Add New**.
4. Type a User ID and password and confirm the password.
5. In the **Permissions Information** section, click **Add to Access Control Group**.
6. In the **Find and List Access Control Groups** window, select the **Admin-3rd Party API** checkbox.
7. Click **Add Selected**.
8. Click **Close** and save.

Create a Dummy User

Use this dummy UDS user to log in to Cisco Unified CM IM and Presence Administration as an end user and get presences of other LDAP end users.

If the customer has configured single sign-on, the dummy user must be synchronized from LDAP directory to the CUCM.

1. Log into Cisco Unified Communications Manager Administration console.
2. Click **User Management > End User**.
3. Click **Add New**.
4. Type a User ID, password, and confirm password for the dummy user account.
5. Select the **Enable User for Unified CM IM and Presence (Configure IM and Presence in the associated UC Service Profile) checklist** to enable the user for presence.
6. Click **Save**.

Configure Cisco Unified Communications Manager and Cisco IM and Presence certificates with the enterprise certificate authority

Cisco Unified Communications Manager (CUCM) and Cisco IM and Presence (CIMP) provide the ability to use multi-server certificates with Subject Alternative Names for tomcat, cup-xmpp, and cup-xmpp-ECDSA services. This topic describes certificate configuration using these recent feature enhancements. Multi-server certificates need only be configured on the CUCM and CIMP Publishers. Regardless of CIMP version, the cup service certificate is not multi-server and must be configured on each CIMP server in the cluster.

If your environment is not using multi-server certificates, you must use the Cisco Operating System Administration user interface on all of the CUCM and CIMP nodes to configure the Tomcat certificates. You must use the Cisco Operating System Administration interface on all of the CIMP nodes to configure the cup, cup-xmpp, and cup-xmpp-ECDSA certificates. The Cisco Tomcat service runs on both CUCM and CIMP servers. The cup, cup-xmpp, and cup-xmpp-ECDSA services only run on the CIMP servers.

When you configure the Presence service to communicate with CUCM and CIMP, you can configure the Cisco certificates to be signed by the enterprise certificate authority. You require the following certificates and certificate signing requests (CSR) when you want to configure the Presence service to communicate with the Cisco Unified Communications Manager and Cisco IM and Presence:

Service	Certificates or CSRs
Configure the Connect service only[1]	• Enterprise Root CA certificate • Tomcat Certificate Signing Request (from CUCM) • Tomcat - CA signed certificate • Tomcat - ECDSA CA signed certificate • Cup-xmpp Certificate Signing Request (from CIMP) • Cup-xmpp CA signed certificate • Cup-ECDSA CA signed certificate (from CIMP) • Cup-xmpp-ECDSA CA signed certificate (from CIMP)

Service	Certificates or CSRs
Configure the Presence service only[1]	• Enterprise Root CA certificate • Tomcat Certificate Signing Request (from CUCM) • Tomcat - CA signed certificate • Tomcat - ECDSA CA signed certificate • Cup Certificate Signing Request (from CIMP) • Cup - CA signed certificate • Cup-ECDSA CA signed certificate (from CIMP) • Cup-xmpp-ECDSA CA signed certificate (from CIMP)

[1] If you configure both the Connect and Presence services, make sure that all of the required certificates or CSRs uploaded.

Note: You must upload the root CA certificate as a trust certificate for the corresponding services or you will receive the error message **CA certificate is not available in the trust-store**. For example, if you want to use a CA-signed tomcat certificate, you must first upload the root CA certificate as a tomcat-trust certificate, if you want to use a CA-signed cup certificate, you must first upload the root CA certificate as a cup-trust certificate, and if you want to use a CA-signed cup-xmpp certificate, you must first upload the root CA certificate as a cup-xmpp-trust certificate.

1. Complete steps 2 to 10 for all of the certificate pairs. For example, tomcat/tomcat-trust, cup/cup-trust, cup-xmpp/cup-xmpp-trust, and cup-xmpp-ECDSA/cup-xmpp-trust.
2. Log in to the **Cisco Unified OS Administration** using your administrator credentials. Complete the following tasks on the CUCM Publisher and the IM and Presence Publisher. For the cup service certificate, complete the following tasks on all servers in the cluster.
3. Click **Security > Certificate Management**.
4. Upload the root enterprise CA certificate.

   The uploaded certificate is distributed to all of the servers in the cluster for the given service (for example, tomcat, cup, cup-xmpp, and cup-xmpp-ECDSA).

   a) Click **Upload Certificate/Certificate chain**.
   b) In the **Certificate Purpose** drop-down list, select the trust store (For example, tomcat-trust, cup-trust, or cup-xmpp-trust).
   c) Click **Browse**. Navigate to the enterprise root certificate downloaded earlier.
   d) Click **Open**.
   e) Click **Upload**.
   f) If the certificate upload is successful, click **Close**.
5. Request a CSR.
   a) Click **Generate CSR**. The new CSR will overwrite the existing CSR for that certificate.
   b) In the **Certificate Purpose** drop-down list, click the service you want to generate the CSR for. For example, tomcat, cup, or cup-xmpp.
   c) In the **Distribution** drop-down list, select **Multi-server (SAN)**.

      Note: Make sure that the list of auto-populated domains in the Subject Alternate Names section contain the FQDNs of the CUCM and CIMP servers that will be configured in BEMS.
   d) Click **Close**. A second copy of the <*service*> certificate appears in the certificate list as a CSR Only type.
   e) Click the CSR Only type version of the <*service*> certificate link.
   f) In the **CSR Details for <*Publisher_Hostname-ms.domain*>,<*service*> certificate** dialog box, click **Download CSR**.
   g) Save the **<*service*>.csr** file. Open the file in a text editor.

h) Copy the certificate information, including the Begin and End Certificate request lines.

6. Paste the new CSR certificate information to the Microsoft Active Directory Certificate Services server.
   a) On the **Microsoft Active Directory Certificate Services** server, click **Request a certificate**.
   b) Click **Advanced certificate request**.
   c) On the **Submit a Certificate Request or Renewal request** window, in the **Saved Request** field, paste the certificate information that you copied in step 5h.
   d) In the **Certificate Template** drop-down list, click **Web Server**.
   e) Click **Submit**.
   f) On the **Certificate Issued** window, select **DER** encoded. Click **Download certificate**.
   g) Click **OK**. By default, the certificate is saved to the Downloads folder.
7. Upload the CA-signed certificate to Cisco Unified Operating System Administration web page to replace the CSR Only version of the appropriate service certificate with the CA-signed version.
   a) On the **Cisco Unified Operating System Administration** web page, click **Upload Certificate/Certificate chain**.
   b) Click **OK**.
   c) Click **Close**. The CSR version of the <*service*> certificate changes to CA-signed.
8. Restart Cisco Services on all IM and Presence nodes.
   a) Log in to the **Cisco Unified IM and Presence Serviceability** server.
   b) Click **Tools > Control Center - Network Services**.
   c) In the **Server** drop-down list, select the IM and Presence server. Click **Go**.
   d) Under **IM and Presence Services**, select **Cisco XCP Router**.
   e) Click **Restart**. Click **OK**.
   f) Click **Tools > Control Center - Feature Service**.
   g) In the **Server** drop-down list, select the IM and Presence server. Click **Go**.
   h) Under **IM and Presence Services**, select **Cisco SIP Proxy**.
   i) Click **Restart**. Click **OK**.
   j) Repeat steps h and i for **Cisco Presence Engine**.
9. Restart the **Cisco Tomcat Service** using SSH on all CUCM and CIMP nodes.
   In a command prompt, type `utils service restart Cisco Tomcat`.

Prerequisites: Docs service

The Docs service requires its own Microsoft SQL Server database. And, while having many of the BEMS core requirements in common, it has additional dependencies not required by the other services.

When you configure the BEMS service, you complete the following additional actions:

- Server software and operation system requirements
- Database requirements
- CMIS requirements

Server software and operating system requirements

In addition to core requirements for all BEMS services, the following prerequisites apply to the Docs service:

Network Capabilities and Resources

- The computer that hosts BEMS must be a domain member and have access to the Microsoft Active Directory.

- Network shares must be accessible from BEMS.
- Microsoft SharePoint sites must be accessible from BEMS.

Database Requirements

A blank Microsoft SQL Server database is required for a new installation of the BlackBerry Docs service. It is recommended that you name the database "BEMS_Docs". The installer extends the schema during the installation process.

If you install the Docs service on a separate computer, two Microsoft SQL Server databases are required. One for the Docs service and one for the BlackBerry Push Notifications It is recommended that you name the databases "BEMS_Docs" and "BEMS_Core4".

CMIS Requirements

Content Management Interoperability Services (CMIS) is an open standard that allows different content management systems to inter-operate over the Internet. The Docs service supports content management systems that support CMIS.

Consult your vendor documentation to determine whether your system is supported by CMIS and whether that support comes via AtomPub or Web Services. If both are supported, Atom Pub is recommended. You must have the binding URL for this support.

Note: Only Microsoft Active Directory users are supported for CMIS. That is, the content management system must be connected to Microsoft Active Directory for user authentication for Docs service to support it.

Prerequisites: BlackBerry Directory Lookup, BlackBerry Follow-Me, and BlackBerry Certificate Lookup services

The BlackBerry Directory Lookup, BlackBerry Follow-Me, and BlackBerry Certificate Lookup services are installed with the BlackBerry Push Notifications (Core and Mail) service and share the same prerequisites.

Installing or upgrading the BEMS software

Install the BEMS software

Before you begin:

- Make sure that you install BEMS on an English implementation of the operating system.
- If your organization uses AlwaysOn support for SQL Server, make sure you complete the steps in Appendix: AlwaysOn Availability support for SQL Server and that you have the FQDN of the AlwaysOn Listener and name of the database that is added to the AlwaysOn Availability Group available before you install the BEMS software. For information about supported SQL Server versions, see the BEMS Compatibility Matrix.
  When you install the BEMS services on separate computers, all steps will not apply. Complete this task on each computer that you install one or more services on.

1. Log in to the computer that you want to install BEMS on using the BEMS service account.
2. Copy the installation files to the computer.
3. Extract the content to a folder on the computer.
4. In the **GoodEnterpriseMobilityServer** installation folder, complete one of the following tasks:
   - If you use an OpenJDK JRE, double-click **InstallBEMS.bat**.
   - If you use Oracle's Java, double-click **GoodEnterpriseMobilityServer.<*version number*>.exe**.

   If a Windows message appears and requests permission for **GoodEnterpriseMobilityServer.<*version number*>.exe** to make changes to the computer, click **Yes**. If a supported version of Java isn't installed on the computer that you are installing BEMS or the JAVA_HOME system variable isn't specified correctly, the error message **Could not find a valid Java virtual machine to load. You may need to reinstall a supported java virtual machine**. For more information on prerequisite requirements, see the Preinstallation checklists. For instructions on setting the JAVA_HOME system variable, see Configure the Java Runtime Environment.
5. In the **BlackBerry Enterprise Mobility Server v<*version number*> setup** screen, in the **Introduction** dialog box, click **Next**.
6. In the **License Agreement** dialog box, select **I accept the terms of the License Agreement**. Click **Next**.
7. In the **Services** dialog box, select the services you want to install. Click **Next**.

   Scroll to the bottom of the page to view all of the service options.
8. In the **Prerequisite** dialog box, click **Next**.

   Note: If the Prerequisite dialog box displays a warning that a prerequisite is not met, you must cancel the installation and complete the prerequisites before you can start the installation again.
9. In the **Host information** dialog box, verify the BEMS Hostname and Domain name. If necessary, select **Modify these values** and type the new Hostname and Domain.
10. Click **Next**.
11. In the **Choose Install Folder** dialog box, click **Next** to accept the default installation folder location.
12. In the **Choose Logs Folder** dialog box, click **Next** to accept the default log file folder location.
13. In the **Administration Information** dialog box, select **This Account (domain/user)** and type the login credentials for the BEMS service account you created in Setting up a Windows service account for BEMS. Click **Next**
14. In the **Database Information** dialog box, perform the following actions:

Task	Steps
Specify the Microsoft SQL Server connection information for the BEMS-Core service database.	**a.** In the **Host** field, type the FQDN and, if applicable, the SQL instance name of your SQL Server. For example, • SQL Express or SQL Server using a SQL Instance name: <*server name*>\<*database instance name*> • SQL Server using the default SQL instance: <*server name*> • If your environment uses AlwaysOn enter the FQDN of the AlwaysOn Listener. **b.** In the **Database name** field, type the name for the BEMS-Core database (for example, if you install of the BEMS services on one server, type `BEMS-Core`. • If you install the BEMS services on separate servers, type one of the following: • If you install the BlackBerry Push Notifications service (Mail service) on one server, type `BEMS-Core1`. • If you install on a server that will host the Presence service, type `BEMS-Core2`. • If you install on a server that will host only the Connect service, type `BEMS-Core3`. • If you install on a server that will host the Connect service and the Presence service together, type `BEMS-Core3`. • If you install on a server that will host only the Docs service, type `BEMS-Core4`. If your environment uses AlwaysOn enter the name of the database that is added to the AlwaysOn Availability Group. **c.** In the **Port** field, type the port number that connects to the SQL Server. If the SQL Server instance is using dynamic ports, leave this field blank. By default, this port is 1433 if a static TCP/IP port is used. **Note:** To use SQL Server dynamic TCP/IP ports, make sure that the SQL Server Browser service is running. **d.** Optionally, in the **Additional Properties** field, specify any connection properties (for example, name1=value1; name2=value2, and so on). For more information, visit docs.microsoft.com to see Setting the connection properties. If your environment uses AlwaysOn with multisubnet deployment, type `MultiSubnetFailover=true`. **e.** By default, the setup application uses SQL Server authentication to connect to the BEMS database. Select **Windows Authentication**. Click **Next**.
Enter the BEMS service account login credentials under which the BEMS-Connect Windows service run.	**a.** In the **Login** field, type the BEMS service account login information (for example, <*domain123*>.example.com\<*BEMS service account username*>). **b.** In the **Password** field, type the BEMS service account password. **c.** Click **Next**.

Task	Steps
Specify the SQL Server connection information for the BEMS-Connect service database.	**a.** In the **Host** field, type the FQDN and, if applicable, the SQL instance name of your SQL Server. For example, • SQL Express or SQL Server using a SQL Instance name: <*server name*>\<*database instance name*> • SQL Server using the default SQL instance : <*server name*> • If your environment uses AlwaysOn enter the FQDN of the AlwaysOn Listener. **b.** In the **Database name** field, type the name for the BEMS-Connect database (for example, if you install the BEMS-Connect service on one server or all of the BEMS services on one server, type `BEMS-Connect`. If your environment uses AlwaysOn enter the name of the database that is added to the AlwaysOn Availability Group. **c.** In the **Port** field, type the port number that connects to the SQL Server. If the SQL Server instance is using dynamic ports, leave this field blank. By default, this port is 1433 if a static TCP/IP port is used. **d.** Optionally, in the **Additional Properties** field, specify any connection properties (for example, name1=value1; name2=value2, and so on). For more information, visit docs.microsoft.com to see Setting the connection properties. If your environment uses AlwaysOn with multi-subnet deployment, type `MultiSubnetFailover=true`. **e.** By default, the setup application uses the SQL Server authentication to connect to the BEMS database. Select **Windows Authentication**. Click **Next**.
Enter the BEMS service account login credentials under which the BEMS-Presence Windows service run. **Note:** A database is not required for the Presence service if all of the BEMS services are installed on one computer.	**a.** In the **Login** field, type the BEMS service account login information (for example, <*domain123*>.example.com\<*BEMS service account username*>). **b.** In the **Password** field, type the BEMS service account password. **c.** Click **Next**.

Task	Steps
Specify the SQL Server connection information for the BEMS-Docs service database.	**a.** In the **Host** field, type the FQDN and, if applicable, the SQL instance name of your SQL Server. For example, • SQL Express or SQL Server using a SQL Instance name: <*server name*>\<*database instance name*> • SQL Server using the default SQL instance : <*server name*> • If your environment uses AlwaysOn enter the FQDN of the AlwaysOn Listener. **b.** In the **Database name** field, type the name for the BEMS-Docs database. For example, BEMS-Docs. • If you install the Docs service with all of the BEMS services on one or on separate computers, type `BEMS-Docs`. If your environment uses AlwaysOn enter the name of the database that is added to the AlwaysOn Availability Group. **c.** In the **Port** field, type the port number that connects to the Microsoft SQL Server. If the SQL Server instance is using dynamic ports, leave this field blank. By default, this port is 1433 if a static TCP/IP port is used. **d.** Optionally, in the **Additional Properties** field, specify any connection properties (for example, name1=value1; name2=value2, and so on). For more information, visit docs.microsoft.com to see Setting the connection properties. If your environment uses AlwaysOn with multi-subnet deployment, type `MultiSubnetFailover=true`. **e.** By default, the setup application uses SQL Server authentication to connect to the BEMS database. Select **Windows Authentication**. **f.** Click **Next**.

15. In the **Pre-installation Summary** dialog box, click **Install** to install BEMS.
16. In the **Installing** dialog box, complete one or more of the following actions
    a) Click **Next** when the BEMS-Mail installation is complete.
    b) Click **Next** when the BEMS-Connect installation is complete.
    c) Click **Next** when the BEMS-Presence installation is complete.
    d) Click **Next** when the BEMS-Docs installation is complete.
17. Optionally, in the **Installing, Upload Credentials** dialog box, you can provide your BlackBerry Online Portal credentials, cluster name and domain name. You can skip this screen and configure this information later in the BEMS Dashboard. Click **Next**.

    If you skip this step during the installation and do not configure the dashboard, you are prompted for this information each time that you upgrade the BEMS instance. Providing this information allows BlackBerry to collect statistical information (for example, the version of BEMS that is installed) and makes uploading the BEMS logs to BlackBerry Technical Support Services easy. For more information about BEMS statistics, see 'Enable upload of BEMS statistics' in the BEMS-Core configuration content.

    a. Click **OK** to enter your credentials. The credentials prepopulate the 'Upload BEMS statistics' and the 'BlackBerry Online Portal Username field' on the 'Log Upload Credentials' screen in the dashboard. For more information, see 'Log Upload Credentials' in the BEMS-Core configuration content.

b. Click **Skip** to continue with the installation. If the **Allow BEMS to send statistics information to BlackBerry** check box is selected and you provide the credentials in the 'Log Upload Credentials' in the dashboard, the 'Upload of BEMS statistics' settings are configured automatically.

18. In the **Install Complete** dialog box, click **Done**.

The setup application opens the BEMS Dashboard at https://localhost:8443/dashboard. By default, the BEMS Dashboard locks after 30 minutes of inactivity.

After you finish: Complete the BEMS configuration in the BEMS dashboard.

Upgrade BEMS

When you upgrade BEMS, you upgrade the existing services only. During the upgrade process you cannot add, change, or remove services. During the upgrade process, notifications are suspended. The BEMS log files, Windows event logs, and the database record the upgrade as BEMS being in maintenance mode. After the upgrade is complete, the log files, event logs, and database show BEMS as being in upgraded mode. A restart of the computer might be required. For more information, see Standard InstallAnywhere Variables.

If you installed the BEMS services on separate computers, complete this task on each computer that you installed a service on. Depending on the services that you install on the computer, some steps might not apply.

Before you begin:

- Make sure you log in with the BEMS service account you created to install BEMS.
- Verify that you have the password for the BEMS service account.
- Stop the Good Technology Common Services on each computer in the cluster that hosts BEMS.
- If you upgrade BEMS in a cluster environment, back up the BEMS cluster database.

1. Log in to the computer that hosts BEMS using your BEMS service account.
2. Copy the installation files to the computer.
3. Extract the contents to a folder on the computer.
4. In the **GoodEnterpriseMobilityServer installation** installation folder, complete one of the following tasks:
   - If you use an OpenJDK JRE, double-click **InstallBEMS.bat**.
   - If you use Oracle's Java, double-click **GoodEnterpriseMobilityServer.<*version number*>.exe**.

   If a Windows message appears and requests permission for **GoodEnterpriseMobilityServer.<*version number*>.exe** to make changes to the computer, click **Yes**. If a supported version of Java isn't installed on the computer that you are installing BEMS or the JAVA_HOME system variable isn't specified correctly, the error message **Could not find a valid Java virtual machine to load. You may need to reinstall a supported java virtual machine**. For more information on prerequisite requirements, see the Preinstallation checklists. For instructions on setting the JAVA_HOME system variable, see Configure the Java Runtime Environment.
5. In the **BlackBerry Enterprise Mobility Server v<*version number*> setup** screen, in the **Introduction** dialog box, select **Upgrade**. Click **Next**.
6. In the **License Agreement** dialog box, select **I accept the terms of the License Agreement**.
7. Click **Next**.
8. In the **Services** dialog box, click **Next**
9. In the **Prerequisite** dialog box, click **Next**.

   Note: If the Prerequisite dialog box displays a warning that a prerequisite is not met, you must cancel the upgrade and complete the prerequisites before you can continue with the upgrade.
10. In the **Host information** dialog box, complete one of the following actions:
    - Select **Use previously installed certificate** to accept the default values and keep the existing certificate.

- Select **Accept these values for Hostname and Domain**, to create the certificate for BEMS.
- Select **Modify these values**, and enter the new hostname and domain.

11. Click **Next**.
12. In the **Choose Install Folder** dialog box, click **Next** to accept the default installation folder location.
13. In the **Choose Logs Folder** dialog box, click **Next** to accept the default log file folder location.
14. In the **Administration Information** dialog box, type the password for the BEMS service account. Click **Next**.
15. In the **AD User Credentials** dialog box, enter the existing BEMS service account login credentials to access the BEMS Dashboard. Click **Next**.
16. In the **Database Information** dialog box, verify the BEMS-Core service database information to connect to the Microsoft SQL Server. Click **Next**.
17. In the **Connect Administrator Information** dialog box, enter the BEMS-Connect service account password. Click **Next**.
18. In the **Connect Database Information** dialog box, verifiy the BEMS-Connect database information to connect to the Microsoft SQL Server. Click **Next**.
19. In the **Presence Administrator Information** dialog box, enter the BEMS-Presence service account password. Click **Next**.
20. In the **Docs Database Information** dialog box, verify the BEMS-Docs database information to connect to the Microsoft SQL Server. Click **Next**.

    If your environment uses AlwaysOn with multi-subnet deployment, in the **Additional Properties** field, type `MultiSubnetFailover=true`.
21. In the **Pre-installation Summary** dialog box, click **Install** to install BEMS.
22. In the **Upgrade Complete** dialog box, complete the following actions:
    a) Click **Next** when the BEMS-Mail upgrade is complete.
    b) Click **Next** when the BEMS-Connect upgrade is complete.
    c) Click **Next** when the BEMS-Presence upgrade is complete.
    d) Click **Next** when the BEMS-Docs upgrade is complete.
23. If you upgraded from a version of BEMS earlier than 2.10 and didn't specify the upload credentials during a previous installation or in the Dashboard, you are prompted in the **Installing, Upload Credentials** dialog box to provide your BlackBerry Online Portal credentials, cluster name and domain name. Click **Next**.

    Providing this information allows BlackBerry to collect statistical information (for example, the version of BEMS that is installed) and makes uploading the BEMS logs to BlackBerry Technical Support Services easy. For more information about BEMS statistics, see 'Enable upload of BEMS statistics' in the BEMS-Core configuration content. Complete one of the following steps:

    - Click **OK** to enter your credentials. The credentials prepopulate the Upload BEMS Statistics and Log Upload Credentials in the dashboard. For more information, see 'Log Upload Credentials' in the BEMS-Core configuration content.
    - Click **Skip** to continue with the installation. If the **Allow BEMS to send statistics information to BlackBerry** check box is selected and you provide the credentials in the 'Log Upload Credentials' in the dashboard, the 'Upload of BEMS statistics' settings are configured automatically.
24. In the **Upgrade Complete** dialog box, complete the following steps:
    a) Verify that the **Start BEMS services** checkbox is selected. If you clear the **Start BEMS services** checkbox, the BEMS installer stops the Good Technology Common Services.
    b) If you are prompted to restart the computer. Select **Yes, restart my system** or **No, I will restart my system myself**.
25. Click **Done**.

After you finish: Configure BEMS. The BEMS Dashboard opens at https://localhost:8443/dashboard.

Perform a Silent Install or Upgrade

You can perform a silent new installation, upgrade, or repair using the silentInstall.bat file or a command prompt. By default, BEMS is installed at the following location: C:\Program Files\BlackBerry\BlackBerry Enterprise Mobility Server.

A template response file **GoodServerSetup.properties** is provided, along with a **silentInstall.bat file** and the BEMS installer, in the installer zip file. The GoodServerSetup.properties file contains the variables and values of the inputs for each screen in the installer for fresh installation, along with instructions on how to edit the variables. The silentInstall.bat file is provided as a convenience to run the silent install command. If you install the BEMS services on separate computers or a custom location (for example, the E drive), modify the GoodServerSetup.properties file accordingly.

Important: If you install, perform an upgrade, or repair a BEMS instance that is not installed in the default location, you must update the USER_INSTALL_DIR1=<*BEMS path*> property in the GoodServerSetup.properties file before you run the silentInstall.bat file. For example, to install BEMS on an E drive using the same folder path, you must complete the following steps:

1. In a text editor, open the GoodServerSetup.properties file.
2. Locate the existing entry "USER_INSTALL_DIR1=C:\\Program Files\\BlackBerry\\BlackBerry Enterprise Mobility Server".
3. Update USER_INSTALL_DIR1: parameter with the custom path (for example, `USER_INSTALL_DIR1=E:\\Program Files\\BlackBerry\\BlackBerry Enterprise Mobility Server`)
4. Save the file.

Double-click **silentInstall.bat file** or in a command prompt, type `<BEMS Installer> LAX_VM "%JAVA_HOME%\bin\java.exe" -i silent -f <response file>`

You can enter Admin-user details, machine details, SQL Server details, and other configuration specifics in this property file and then install the BEMS server in an unattended mode.

Installation results are logged in the install log file folder (for example, `<drive>:\Users\<alias>\AppData\Local\good`). Where <*alias*> is the name of the admin user account.

This silent install feature also can be used to upgrade or repair/modify the server. A password can be specified as part of the command file.

Removing the BEMS software

When you stop a BEMS instance, it will not be used by your high availability implementation, and all users that are serviced by the discontinued instance are reallocated to other servers automatically as soon as the discontinued instance goes down. This also applies to BlackBerry Connect server instances. If you installed the BEMS services on separate computers, complete these tasks on each computer that hosts the BEMS services.

After the BEMS software is removed, other BEMS instances check the BEMS databases (for example, BEMS-Core and BEMS-Connect) for instances that have not checked in within the default number of days. Inactive server references are removed from the databases automatically.

- For BEMS instances that were installed with the BEMS-Core, Mail, Docs, or Presence services, the default inactive time period is 30 days.
- For BEMS instances that were installed with the Connect service, the default inactive time period is three days.

1. Remove the BEMS software.
2. Complete one of the following actions:
   - In a BlackBerry UEM environment, remove the BEMS server references from the BlackBerry Dynamics connectivity profile.
   - In a Good Control environment, remove the BEMS server references for BlackBerry Work.
3. Remove the BEMS Connect server references for BlackBerry Connect.

Remove the BEMS software

Complete one of the following tasks on the computer that hosts BEMS:

Remove method	Steps
Installer	**a.** Navigate to the installation folder. By default, the installation folder is located at <*BEMS_install_location*>\GoodEnterpriseMobilityServerSetup.<*version*>.exe. **b.** Double-click **GoodEnterpriseMobilityServer.<*version number*>.exe**. **c.** Select **Uninstall** and follow the instructions on the screen.
Windows menu	**a.** Click Start > **BlackBerry Enterprise Mobility Server > Change BlackBerry Enterprise Mobility Server Installation**. **b.** Click **Uninstall**. **c.** Click **Uninstall BlackBerry Enterprise Mobility Server** to confirm that you want to uninstall the software. **d.** Click **Done**.

In a BlackBerry UEM environment, remove the BEMS server references from the BlackBerry Dynamics connectivity profile

1. In the BlackBerry UEM management console, on the menu bar, click **Policies and profiles.**
2. Click **Networks and connections > BlackBerry Dynamics connectivity profile**.
3. Click the BlackBerry Dynamics connectivity profile that you want to remove the BEMS instance from.

4. Click .
5. If specified, in the **Additional servers** section, remove the BEMS instances.
6. If specified, in the **IP address ranges** section, remove the BEMS instances.
7. In the **App servers** section, if listed locate the BlackBerry Work app entitlement.
8. Click ✕ beside the instance that has been decommissioned.
9. Repeat steps 7 and 8 for the following entitlements that might be listed:
   - Good Enterprise Services (com.good.gdserviceentitlement.enterprise)
   - BlackBerry Connect (com.good.goodconnect)
   - Feature-Docs Service Entitlement (com.good.feature.share)
   - BlackBerry Core and Mail Services (com.blackberry.gdserviceentitlement.coreandmail)
   - BlackBerry Presence Service (com.blackberry.gdservice.entitlement.presence)
   - BlackBerry Tasks (com.blackberry.gd.tasks)
   - BlackBerry Notes (com.blackberry.gd.notes)
10. Click **Remove** beside any additional entitlements that do not have a BEMS instance associated with them.

    Note: Only complete this step if a BEMS instance is no longer required in your environment for BlackBerry Dynamics apps.
11. Click **Save**.

In a Good Control environment, remove the BEMS server references for BlackBerry Work

1. Uninstall the BEMS instance on the host machine.
2. In Good Control, under **Apps**, click **Manage Apps**.
3. Click **BlackBerry Work**.
4. Click the **BlackBerry Dynamics** tab.
5. In the **Server** section, click **Edit**.
6. Click the BEMS server that you want to remove. Click .
7. Click **Save**.

Remove the BEMS Connect server references for BlackBerry Connect

1. In a BlackBerry UEM environment, complete the following steps:
   a) Log in to the BlackBerry UEM console.
   b) On the menu, click **Apps**.
   c) Search for and click the BlackBerry Connect app.
   d) On the **Settings > BlackBerry Dynamics** tab, in the **App configuration** section, click the App Configuration you want to remove the BEMS instance from.
   e) On the **Server Configuration** tab, remove the BEMS instance from the Connect Server Hosts table. For more information, see "Configure BlackBerry Connect app settings in BlackBerry UEM" in the BlackBerry Connect administration content.
2. In a Good Control environment, complete the following steps:
   a) Uninstall the BEMS instance on the host machine.
   b) In Good Control, under **Apps**, click **Manage Apps**.

c) Click **Good Connect**.
d) Click the **BlackBerry Dynamics** tab.
e) In the **Server** section, click **Edit**.
f) Click the BEMS server you want to remove. Click .

3. Click **Save**.

Troubleshooting BEMS installation or upgrade

In some cases you might need to troubleshoot a BEMS installation or upgrade issue. In some cases you might need to return BEMS to the previous version of the software and then retry the upgrade. The approach to take depends on the current state of your environment and the BEMS software versions involved in the upgrade.

For detailed information about the data (for example, BEMS installation logs) that must be captured to assist in troubleshooting and resolving BEMS installation and upgrade issues, visit support.blackberry.com/community to read article 51187.

Appendices

Appendix: AlwaysOn Availability support for SQL Server

The AlwaysOn Availability Groups feature is a high-availability and disaster-recovery solution that provide an enterprise-level alternative to database mirroring. Introduced in SQL Server 2012, AlwaysOn Availability Groups maximize the availability of a set of user databases for an enterprise that is running SQL Server 2012, 2014, 2016, or 2017. An availability group supports a failover environment for a discrete set of user databases, known as availability databases, that fail over together. A read-scale availability group is a group of databases that perform read-only work and are copied from other SQL Server instances.

An availability group supports a set of read-write primary databases and one to eight sets of corresponding secondary databases. Optionally, secondary databases can be made available for read-only access and some backup operations.

For more information about AlwaysOn availability, visit docs.microsoft.com to read Overview of Always On Availabilty Groups.

Steps to setup SQL Server for AlwaysOn availability

When you setup SQL Serverfor AlwaysOn availability, you perform the following actions:

Step	Action
1	Create an AlwaysOn availability group.
2	Configure SQL Server for AlwaysOn availability.
3	Install the BEMS software.
4	Configure the BEMS services databases for AlwaysOn availability.
5	Configure AlwaysOn availability group failover for single and multi-subnets for the following services: • Core and Mail • Connect • Docs

Configure the BEMS services databases for AlwaysOn availability

Complete this task if you installed BEMS in your environment without specifying the server and database for AlwaysOn during the installation. Complete these steps on each BEMS instance in your environment.

Note: If you manually specify the AlwaysOn Listener and database name in the BEMS dashboard, you must specify the updated server and database information when you perform future upgrades. For instructions on upgrading BEMS, see Upgrade BEMS.

Important: To install BEMS services connected to a database in AlwaysOn, the instance name must be set to the Listener in the AlwaysOn group, not the cluster name and not the host name of the host server in the cluster.

Before you begin: The databases created for BEMS services need to be added into the AlwaysOn group.

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BlackBerry Services Configuration**, click **Mail**.
2. Click **Database**.
3. In the **Server** field, enter the FQDN of the AlwaysOn Listener.
4. In the **Database** field, enter the name of the database that is added to the AlwaysOn Availability Group.
5. Click **Test** to test the connection.
6. Click **Save**.
7. Repeat steps 1 to 7 for the Connect and Docs services.

Enabling AlwaysOn availability group failover to subnets for the BEMS-Core and Mail services

You can enable availability group failovers to different subnets by setting MultiSubnetFailover to true for the BEMS-Core and Mail services. You can set this option if you have single and multi-subnet connections. For more information about subnet failovers, visit docs.microsoft.com to read Listeners, clients and failover.

For instructions on enabling AlwaysOn availability group failover to subnets for the BEMS-Core and Mail services when installing a new BEMS or upgrading a BEMS instance, see the following:

- During a new installation, see Install the BEMS software.
- During an upgrade, see Upgrade BEMS.

Enabling AlwaysOn availability group failover to subnets for the Connect service

You can enable availability group failovers to different subnets during BEMS installation, upgrade, and repair processes. You can set this option if you have single and multi-subnet connections. For more information about subnet failovers, see the Microsoft Documentation to read Listeners, clients and failover.

For instructions on enabling AlwaysOn availability group failover to subnets for the Connect service when installing a new BEMS or upgrading a BEMS instance, see the following:

- During a new installation, see Install the BEMS software.
- During an upgrade, see Upgrade BEMS.

Enabling AlwaysOn availability group failover to subnets for the Docs service

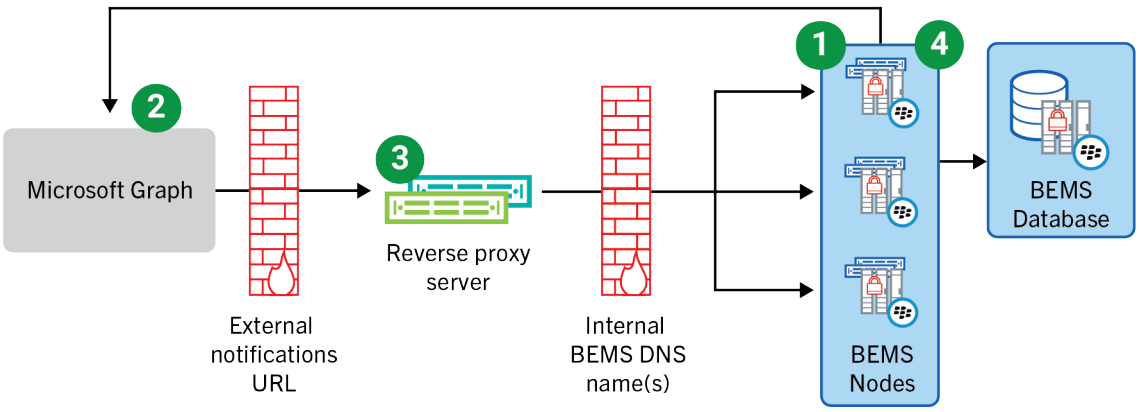
You can enable AlwaysOn availability group failover to subnets for the Docs service during the BEMS installation, upgrade, and repair processes. For instructions on enabling AlwaysOn availability group failover to subnets for the Docs service when installing a new BEMS or upgrading a BEMS instance, see the following:

- During a new installation, see Install the BEMS software.
- During an upgrade, see Upgrade BEMS.

Architecture: BEMS notification flow using the Microsoft Graph API

In 2022, Microsoft started to deprecate the Microsoft Exchange Web Services (EWS) for Microsoft Microsoft Exchange Online APIs replacing the EWS with Microsoft Graph. For more information, visit techcommunity.microsoft.com and read 'Upcoming API Deprecations in Exchange Web Services for Exchange Online'.

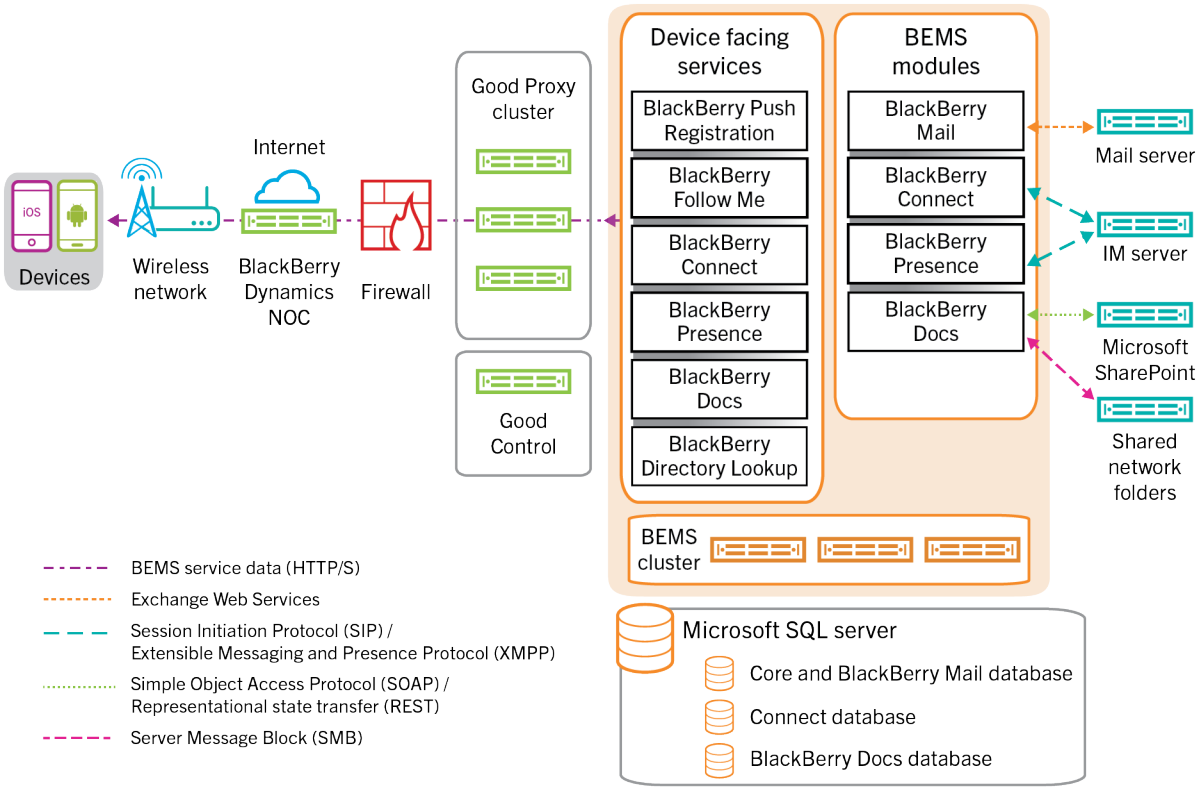
This diagram shows how BEMS uses Microsoft Graph to send notifications to devices.



Component name	Description
BEMS	BEMS consolidates several BEMS services used to send work data to and from BlackBerry Dynamics apps, including BlackBerry Push Notifications (BlackBerry Mail), BlackBerry Connect, BlackBerry Presence, and BlackBerry Docs. BEMS listens for notification URI sent by the Microsoft Graph API.
Reverse proxy server	The reverse proxy server receives the Microsoft Graph connection and forwards the connection to the private BEMS URI.
Microsoft Graph	Microsoft Graph is a RESTful web API that allows you to communicate with Microsoft Cloud service resources.

1. In the BEMS console (Mail > Microsoft Graph), you add the External Notification URL that the Microsoft Graph API will use to initiate connections to the reverse proxy server.
2. The Microsoft Graph API initiates connections to your organization's reverse proxy using the provided External Notifications URL.
3. The reverse proxy server intercepts the Microsoft Graph connection request and translates/routes the connection request to your private BEMS instance.
4. BEMS receives the request from the reverse proxy and sends the new notification to the user's BlackBerry Dynamics app (for example, BlackBerry Work) based on the notification rules and configuration set for the user.

Architecture: BEMS

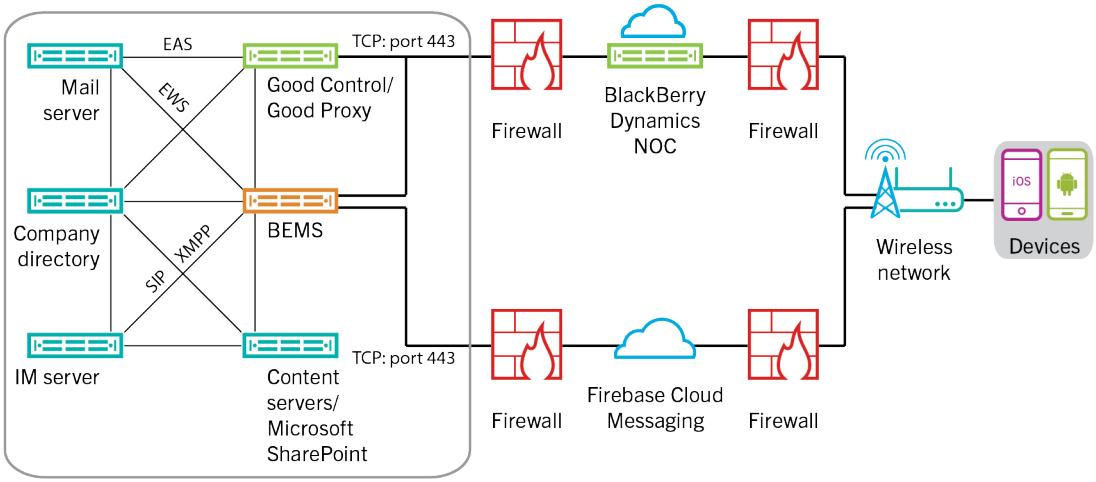


From this high-level architectural view, the diagram does not show how the BlackBerry Work application connects to Microsoft Exchange Server for accessing email. It shows how each BEMS service is accessed by BlackBerry Work on devices, which is BEMS role, to expose secure device-facing services used by BlackBerry Work and make them available to other BlackBerry Dynamics-powered apps. These services currently include BlackBerry Push Registration, BlackBerry Follow Me, BlackBerry Presence, BlackBerry Directory Lookup, and BlackBerry Docs.

Communicating using the protocols shown, the feature modules of BEMS integrate with your backend systems of record using a shared Microsoft SQL Server running multiple databases for Core/Mail, Connect, and Docs.

For high availability, BEMS is deployed as a cluster, with all of its device-facing services provided by all instances of BEMS in the cluster and made available to client devices through the BlackBerry Dynamics infrastructure. Each BlackBerry Dynamics-powered client app connects through a Good Proxy cluster deployed on-premise. Entitlement to use BEMS services is managed through Good Control.

A slightly different view looks like this again at a high level:



It is important to note in the diagram above that the BlackBerry Mail service utilizes the same database server as Good Control. The database server can be local to Good Control or remote.

Some necessary supporting infrastructure is required to support enterprise network operations. Such components include:

- Microsoft Exchange Server
- Skype for Business
- Cisco Unified Communications Manager for IM and Presence
- Microsoft Active Directory
- Good Control
- Good Proxy

For more information about the BEMS architecture in a BlackBerry UEM environment, see the BlackBerry UEM Architecture and Data Flow Reference content.

Legal notice

©2023 BlackBerry Limited. Patents, as applicable, identified at: www.blackberry.com/patents Trademarks, including but not limited to BLACKBERRY, BBM, BES, EMBLEM Design, ATHOC, CYLANCE and SECUSMART are the trademarks or registered trademarks of BlackBerry Limited, its subsidiaries and/or affiliates, used under license, and the exclusive rights to such trademarks are expressly reserved. All other trademarks are the property of their respective owners.

Patents, as applicable, identified at: www.blackberry.com/patents.

This documentation including all documentation incorporated by reference herein such as documentation provided or made available on the BlackBerry website provided or made accessible "AS IS" and "AS AVAILABLE" and without condition, endorsement, guarantee, representation, or warranty of any kind by BlackBerry Limited and its affiliated companies ("BlackBerry") and BlackBerry assumes no responsibility for any typographical, technical, or other inaccuracies, errors, or omissions in this documentation. In order to protect BlackBerry proprietary and confidential information and/or trade secrets, this documentation may describe some aspects of BlackBerry technology in generalized terms. BlackBerry reserves the right to periodically change information that is contained in this documentation; however, BlackBerry makes no commitment to provide any such changes, updates, enhancements, or other additions to this documentation to you in a timely manner or at all.

This documentation might contain references to third-party sources of information, hardware or software, products or services including components and content such as content protected by copyright and/or third-party websites (collectively the "Third Party Products and Services"). BlackBerry does not control, and is not responsible for, any Third Party Products and Services including, without limitation the content, accuracy, copyright compliance, compatibility, performance, trustworthiness, legality, decency, links, or any other aspect of Third Party Products and Services. The inclusion of a reference to Third Party Products and Services in this documentation does not imply endorsement by BlackBerry of the Third Party Products and Services or the third party in any way.

EXCEPT TO THE EXTENT SPECIFICALLY PROHIBITED BY APPLICABLE LAW IN YOUR JURISDICTION, ALL CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS, OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS OR WARRANTIES OF DURABILITY, FITNESS FOR A PARTICULAR PURPOSE OR USE, MERCHANTABILITY, MERCHANTABLE QUALITY, NON-INFRINGEMENT, SATISFACTORY QUALITY, OR TITLE, OR ARISING FROM A STATUTE OR CUSTOM OR A COURSE OF DEALING OR USAGE OF TRADE, OR RELATED TO THE DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN, ARE HEREBY EXCLUDED. YOU MAY ALSO HAVE OTHER RIGHTS THAT VARY BY STATE OR PROVINCE. SOME JURISDICTIONS MAY NOT ALLOW THE EXCLUSION OR LIMITATION OF IMPLIED WARRANTIES AND CONDITIONS. TO THE EXTENT PERMITTED BY LAW, ANY IMPLIED WARRANTIES OR CONDITIONS RELATING TO THE DOCUMENTATION TO THE EXTENT THEY CANNOT BE EXCLUDED AS SET OUT ABOVE, BUT CAN BE LIMITED, ARE HEREBY LIMITED TO NINETY (90) DAYS FROM THE DATE YOU FIRST ACQUIRED THE DOCUMENTATION OR THE ITEM THAT IS THE SUBJECT OF THE CLAIM.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, IN NO EVENT SHALL BLACKBERRY BE LIABLE FOR ANY TYPE OF DAMAGES RELATED TO THIS DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN INCLUDING WITHOUT LIMITATION ANY OF THE FOLLOWING DAMAGES: DIRECT, CONSEQUENTIAL, EXEMPLARY, INCIDENTAL, INDIRECT, SPECIAL, PUNITIVE, OR AGGRAVATED DAMAGES, DAMAGES FOR LOSS OF PROFITS OR REVENUES, FAILURE TO REALIZE ANY EXPECTED SAVINGS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, LOSS OF BUSINESS OPPORTUNITY, OR CORRUPTION OR LOSS OF DATA, FAILURES TO TRANSMIT OR RECEIVE ANY DATA, PROBLEMS ASSOCIATED WITH ANY APPLICATIONS USED IN CONJUNCTION WITH BLACKBERRY PRODUCTS OR SERVICES, DOWNTIME COSTS, LOSS OF THE USE OF BLACKBERRY PRODUCTS OR SERVICES OR ANY PORTION THEREOF OR OF ANY AIRTIME SERVICES, COST OF SUBSTITUTE GOODS, COSTS OF COVER, FACILITIES OR

SERVICES, COST OF CAPITAL, OR OTHER SIMILAR PECUNIARY LOSSES, WHETHER OR NOT SUCH DAMAGES WERE FORESEEN OR UNFORESEEN, AND EVEN IF BLACKBERRY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, BLACKBERRY SHALL HAVE NO OTHER OBLIGATION, DUTY, OR LIABILITY WHATSOEVER IN CONTRACT, TORT, OR OTHERWISE TO YOU INCLUDING ANY LIABILITY FOR NEGLIGENCE OR STRICT LIABILITY.

THE LIMITATIONS, EXCLUSIONS, AND DISCLAIMERS HEREIN SHALL APPLY: (A) IRRESPECTIVE OF THE NATURE OF THE CAUSE OF ACTION, DEMAND, OR ACTION BY YOU INCLUDING BUT NOT LIMITED TO BREACH OF CONTRACT, NEGLIGENCE, TORT, STRICT LIABILITY OR ANY OTHER LEGAL THEORY AND SHALL SURVIVE A FUNDAMENTAL BREACH OR BREACHES OR THE FAILURE OF THE ESSENTIAL PURPOSE OF THIS AGREEMENT OR OF ANY REMEDY CONTAINED HEREIN; AND (B) TO BLACKBERRY AND ITS AFFILIATED COMPANIES, THEIR SUCCESSORS, ASSIGNS, AGENTS, SUPPLIERS (INCLUDING AIRTIME SERVICE PROVIDERS), AUTHORIZED BLACKBERRY DISTRIBUTORS (ALSO INCLUDING AIRTIME SERVICE PROVIDERS) AND THEIR RESPECTIVE DIRECTORS, EMPLOYEES, AND INDEPENDENT CONTRACTORS.

IN ADDITION TO THE LIMITATIONS AND EXCLUSIONS SET OUT ABOVE, IN NO EVENT SHALL ANY DIRECTOR, EMPLOYEE, AGENT, DISTRIBUTOR, SUPPLIER, INDEPENDENT CONTRACTOR OF BLACKBERRY OR ANY AFFILIATES OF BLACKBERRY HAVE ANY LIABILITY ARISING FROM OR RELATED TO THE DOCUMENTATION.

Prior to subscribing for, installing, or using any Third Party Products and Services, it is your responsibility to ensure that your airtime service provider has agreed to support all of their features. Some airtime service providers might not offer Internet browsing functionality with a subscription to the BlackBerry® Internet Service. Check with your service provider for availability, roaming arrangements, service plans and features. Installation or use of Third Party Products and Services with BlackBerry's products and services may require one or more patent, trademark, copyright, or other licenses in order to avoid infringement or violation of third party rights. You are solely responsible for determining whether to use Third Party Products and Services and if any third party licenses are required to do so. If required you are responsible for acquiring them. You should not install or use Third Party Products and Services until all necessary licenses have been acquired. Any Third Party Products and Services that are provided with BlackBerry's products and services are provided as a convenience to you and are provided "AS IS" with no express or implied conditions, endorsements, guarantees, representations, or warranties of any kind by BlackBerry and BlackBerry assumes no liability whatsoever, in relation thereto. Your use of Third Party Products and Services shall be governed by and subject to you agreeing to the terms of separate licenses and other agreements applicable thereto with third parties, except to the extent expressly covered by a license or other agreement with BlackBerry.

The terms of use of any BlackBerry product or service are set out in a separate license or other agreement with BlackBerry applicable thereto. NOTHING IN THIS DOCUMENTATION IS INTENDED TO SUPERSEDE ANY EXPRESS WRITTEN AGREEMENTS OR WARRANTIES PROVIDED BY BLACKBERRY FOR PORTIONS OF ANY BLACKBERRY PRODUCT OR SERVICE OTHER THAN THIS DOCUMENTATION.

BlackBerry Enterprise Software incorporates certain third-party software. The license and copyright information associated with this software is available at http://worldwide.blackberry.com/legal/thirdpartysoftware.jsp.

BlackBerry Limited
2200 University Avenue East
Waterloo, Ontario
Canada N2K 0A7

BlackBerry UK Limited
Ground Floor, The Pearce Building, West Street,
Maidenhead, Berkshire SL6 1RL
United Kingdom

Published in Canada